ESET ENDPOINT SECURITY 6

Guia do Usuário

Microsoft® Windows® 10/8.1/8/7/Vista/XP x86 SP3/XP x64 SP2

Clique aqui para fazer download da versão mais recente deste documento

ESET ENJOY SAFER TECHNOLOGY™

ESET ENDPOINT SECURITY 6

Atendimento ao cliente mundial www.eset.com/support

REV. 9/3/2015

Índice

Índice

1. ESET Endpoint Security

O ESET Endpoint Security 6 representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento ThreatSense®, combinada com o firewall pessoal personalizado e o módulo antispam, utiliza velocidade e precisão para manter o computador seguro. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e programas maliciosos que podem comprometer o funcionamento do computador.

O ESET Endpoint Security 6 é uma solução de segurança completa desenvolvida a partir do nosso esforço de longo prazo para combinar proteção máxima e impacto mínimo no sistema. As tecnologias avançadas, com base em inteligência artificial, são capazes de eliminar proativamente a infiltração por vírus, spywares, cavalos de troia, worms, adwares, rootkits e outros ataques via Internet sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

O ESET Endpoint Security 6 foi projetado principalmente para o uso em estações de trabalho em um ambiente de negócios/empresarial. É possível usá-lo com o ESET Remote Administrator, permitindo gerenciar facilmente qualquer número de estações de trabalho do cliente, aplicar políticas e regras, monitorar detecções e configurar remotamente a partir de qualquer computador em rede.

1.1 O que há de novo

A interface gráfica do usuário do ESET Endpoint Security foi totalmente reformulada para fornecer melhor visibilidade e uma experiência mais intuitiva para o usuário. Algumas das muitas melhorias incluídas no ESET Endpoint Security versão 6 incluem:

Melhorias funcionais e de utilização

- Controle de Web - Define uma única regra para vários URLs ou define diferentes políticas para diferentes locais de rede. Políticas de bloqueio de software são novas na versão 6, além da capacidade de personalizar parcialmente a página de bloqueios e avisos.
- Firewall pessoal - Agora você pode criar regras de firewall diretamente da janela de notificação de IDS ou log e atribuir perfis para interfaces de rede.
- Uma nova proteção contra botnet - ajuda a descobrir malware ao analisar seus padrões e protocolos de comunicação de rede.
- Controle de dispositivos - Agora inclui a capacidade de terminar o tipo de dispositivo e número de série, bem como definir regras individuais para vários dispositivos.
- Um novo Modo interativo para HIPS - está entre o modo Automático e Interativo. Capacidade de identificar atividades suspeitas e processos maliciosos no sistema.
- Melhorias no atualizador/imagem - Agora você pode retomar downloads que falharam do banco de dados de assinatura de vírus e/ou módulos de produto.
- Nova abordagem para capacidade de gerenciamento remoto para seus computadores com o ESET Remote Administrator - Reenvie logs no caso de uma reinstalação do ERA ou testes, instalação remota de soluções de segurança da ESET, para obter uma visão geral do estado de segurança de seu ambiente em rede e classificar vários dados para uso posterior.
- Melhorias na interface do usuário - Adiciona a opção de um clique para executar uma atualização manual do banco de dados de assinatura de vírus e módulos da bandeja do sistema do Windows. Compatível com monitores de alta resolução e telas de toque.
- Detecção aprimorada e remoção de soluções de segurança de terceiros.

Nova funcionalidade

- Antiphishing - Outra camada de proteção que fornece um nível superior de defesa de sites ilegítimos que tentam adquirir senhas e outras informações confidenciais.
- Melhorias na velocidade de rastreamento - usando cache local compartilhado em ambientes virtualizados.

Tecnologias de detecção e proteção

- Velocidade de instalação e confiabilidade aprimoradas.
- Scanner de memória avançado - Monitora o comportamento do processo e rastreia processos maliciosos quando eles ocorrem na memória.
- Bloqueio de exploit aprimorado - Feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. O Bloqueio de Exploit agora tem suporte a Java e ajuda a melhorar a detecção de e proteção contra esses tipos de vulnerabilidades.
- Detecção e remoção de rootkits aprimoradas.
- Escudo de vulnerabilidade - Opções de filtragem mais avançadas para detectar vários tipos de ataques e vulnerabilidades.
- Scanner no estado ocioso - Um rastreamento sem segundo plano do computador será realizado em todas as unidades locais.

1.2 Requisitos do sistema

Para uma operação sem interrupções do ESET Endpoint Security, o sistema deve atender aos seguintes requisitos de hardware e de software:

Processadores compatíveis: Intel® ou AMD x86-x64

Sistemas operacionais: Microsoft® Windows® 8.1/8/7/Vista/XP SP3 32-bit/XP SP2 64-bit

1.3 Prevenção

Quando você trabalhar com o computador, e especialmente quando navegar na Internet, tenha sempre em mente que nenhum sistema antivírus do mundo pode eliminar completamente o risco de infiltrações e ataques. Para fornecer proteção e conveniência máximas, é essencial usar a solução antivírus corretamente e aderir a diversas regras úteis:

Atualização regular

De acordo com as estatísticas do ESET Live Grid, milhares de novas ameaças únicas são criadas todos os dias a fim de contornar as medidas de segurança existentes e gerar lucro para os seus autores - todas às custas dos demais usuários. Os especialistas no Laboratório de vírus da ESET analisam essas ameaças diariamente, preparam e publicam atualizações a fim de melhorar continuamente o nível de proteção de nossos usuários. Para garantir a máxima eficácia dessas atualizações, é importante que elas sejam configuradas devidamente em seu sistema. Para obter mais informações sobre como configurar as atualizações, consulte o capítulo Configuração da atualização.

Download dos patches de segurança

Os autores dos softwares maliciosos frequentemente exploram as diversas vulnerabilidades do sistema a fim de aumentar a eficiência da disseminação do código malicioso. Considerado isso, as empresas de software vigiam de perto quaisquer vulnerabilidades em seus aplicativos para elaborar e publicar atualizações de segurança, eliminando as ameaças em potencial regularmente. É importante fazer o download dessas atualizações de segurança à medida que são publicadas. Microsoft Windows e navegadores da web, como o Internet Explorer, são dois exemplos de programas para os quais atualizações de segurança são lançadas regularmente.

Backup de dados importantes

Os escritores dos softwares maliciosos não se importam com as necessidades dos usuários, e a atividade dos programas maliciosos frequentemente leva ao mau funcionamento de um sistema operacional e à perda de dados importantes. É importante fazer o backup regular dos seus dados importantes e sensíveis para uma fonte externa como um DVD ou disco rígido externo. Isso torna mais fácil e rápido recuperar os seus dados no caso de falha do sistema.

Rastreie regularmente o seu computador em busca de vírus

A detecção de mais vírus, cavalos de troia e rootkits conhecidos e desconhecidos é realizada pelo módulo Proteção em tempo real do sistema de arquivos. Isso significa que sempre que você acessar ou abrir um arquivo, ele será

rastreado quanto à atividade de malware. Recomendamos que você execute um rastreamento no computador inteiro pelo menos uma vez por mês, pois a assinatura de malware varia, assim como as atualizações do banco de dados de assinatura de vírus são atualizadas diariamente.

Siga as regras básicas de segurança

Essa é a regra mais útil e eficiente de todas - seja sempre cauteloso. Hoje, muitas ameaças exigem a interação do usuário para serem executadas e distribuídas. Se você for cauteloso ao abrir novos arquivos, economizará tempo e esforço consideráveis que, de outra forma, seriam gastos limpando as ameaças. Aqui estão algumas diretrizes úteis:

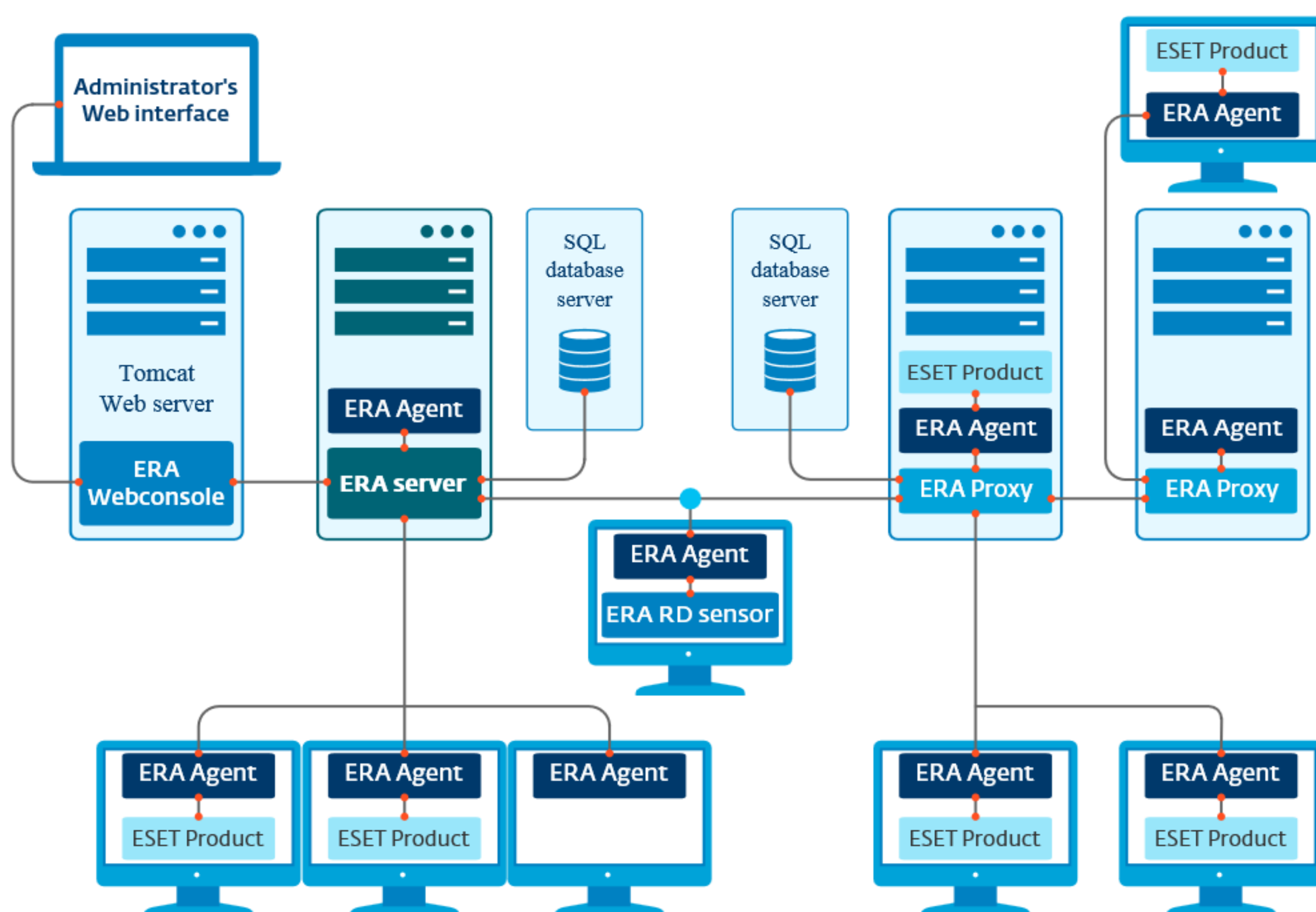
- Não visite sites suspeitos com inúmeras pop-ups e anúncios piscando.
- Seja cuidadoso ao instalar programas freeware, pacotes codec. etc. Use somente programas seguros e somente visite sites da Internet seguros.
- Seja cauteloso ao abrir anexos de e-mail, especialmente aqueles de mensagens spam e mensagens de remetentes desconhecidos.
- Não use a conta do Administrador para o trabalho diário em seu computador.

2. Documentação para usuários conectados via ESET Remote Administrator

ESET Remote Administrator (ERA) é um aplicativo que permite que você gerencie produtos ESET em um ambiente em rede a partir de um local central. O sistema de gerenciamento de tarefas do ESET Remote Administrator permite que você instale soluções de segurança da ESET em computadores remotos e responda rapidamente a novos problemas e ameaças. O ESET Remote Administrator não fornece proteção contra código malicioso por si só, ele conta com a presença de uma solução de segurança da ESET em cada cliente.

As soluções de segurança da ESET são compatíveis com redes que incluem vários tipos de plataforma. Sua rede pode incluir uma combinação de sistemas operacionais Microsoft, Linux e Mac OS que são executados em dispositivos móveis (celulares e tablets).

A imagem a seguir mostra uma arquitetura de exemplo para uma rede protegida por soluções de segurança da ESET gerenciada por ERA:



OBSERVAÇÃO: Para obter mais informações, consulte o Guia do usuário do ESET Remote Administrator.

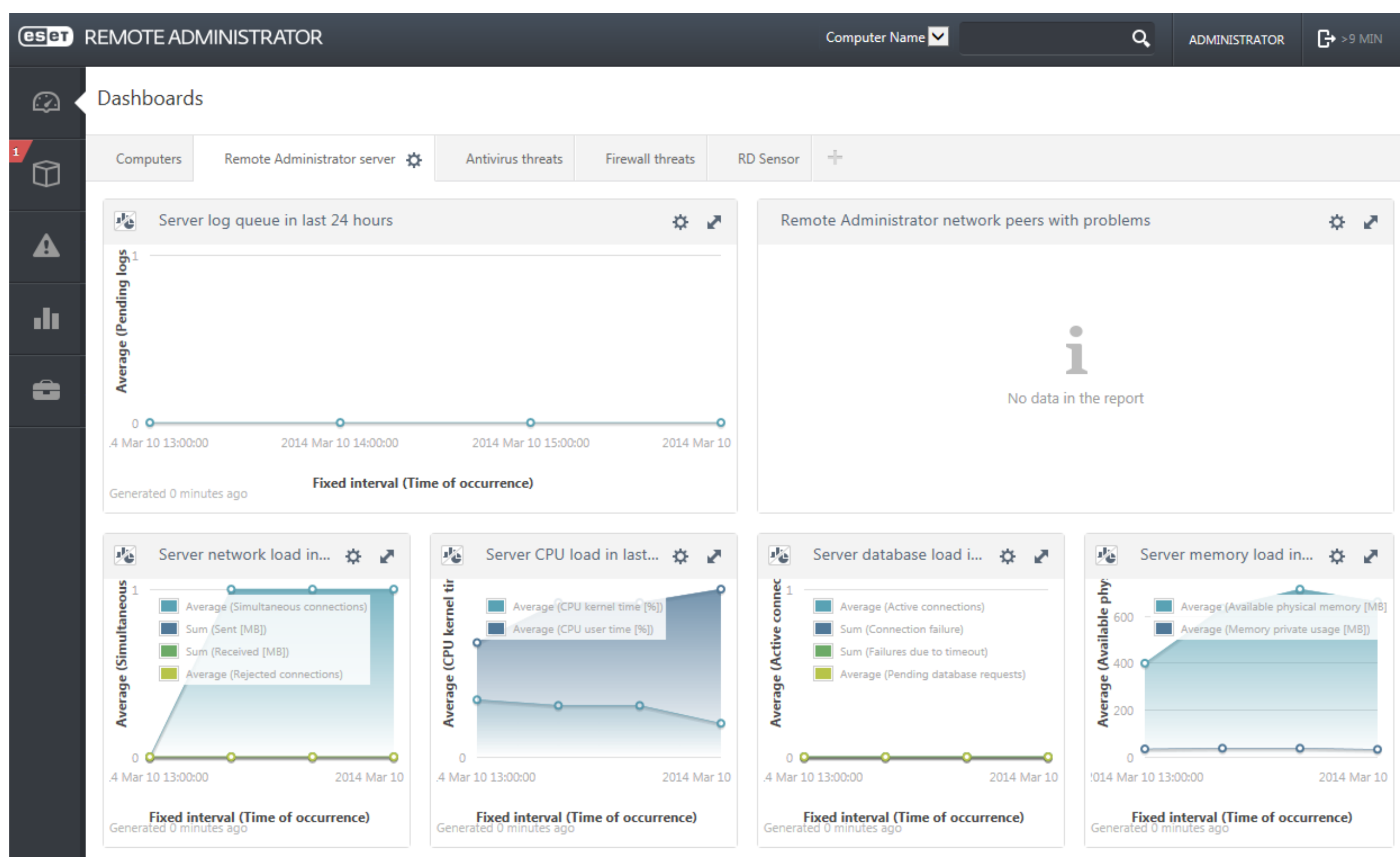
2.1 Servidor do ESET Remote Administrator

Servidor do ESET Remote Administrator é um componente primário do ESET Remote Administrator. Ele é o aplicativo executivo que processa todos os dados recebidos de clientes que se conectam ao Servidor (por meio do Agente ERA). O Agente ERA facilita a comunicação entre o cliente e o servidor. Dados (relatórios de cliente, configuração, replicação do agente, etc.) são armazenados em um banco de dados. Para processar dados corretamente, o Servidor ERA exige uma conexão estável com um servidor de banco de dados. Recomendamos que você instale o Servidor ERA e seu banco de dados em servidores separados para otimizar o desempenho. A máquina na qual o Servidor ERA está instalado deve ser configurada para aceitar todas as conexões de Agente/Proxy/RD Sensor, que são verificadas usando certificados. Quando instalado, você pode abrir o Console da Web ERA que se conecta aos Servidor ERA (como pode ser visto no diagrama). A partir do console da Web, todas as operações do Servidor ERA são realizadas enquanto se gerencia as soluções de segurança ESET dentro da sua rede.

2.2 Console da web

O **ERA console da Web** é uma interface de usuário na Web que apresenta dados do Servidor ERA e permite que você gerencie as soluções de segurança da ESET em seu ambiente. O Console da Web pode ser acessado usando um navegador. Ele exibe uma visão geral do status de clientes em sua rede e pode ser usado para implantar remotamente soluções da ESET em computadores não gerenciados. Você pode escolher tornar o servidor Web acessível pela internet, para permitir o uso do ESET Remote Administrator de praticamente qualquer lugar ou dispositivo.

Este é o Painel do console da Web:



A ferramenta **Pesquisa rápida** está localizada na parte superior do console da Web. Selecione **Nome do computador**, **Endereço IPv4/IPv6** ou **Nome da ameaça** no menu suspenso, digite sua sequência de pesquisa no campo de texto e clique no símbolo da lente de aumento ou pressione **Enter** para pesquisar. Você será redirecionado para a seção **Grupos**, onde seu resultado de pesquisa será exibido.

OBSERVAÇÃO: Para obter mais informações, consulte o Guia do usuário do ESET Remote Administrator.

2.3 Proxy

Proxy ERA é outro componente do ESET Remote Administrator e atende a duas finalidades. No caso de uma rede de médio porte ou corporativa com muitos clientes (por exemplo, 10.000 clientes ou mais), você pode usar o Proxy ERA para distribuir a carga entre vários Proxies ERA, facilitando para o Servidor ERA principal. A outra vantagem do Proxy ERA é que você pode usá-lo ao se conectar a uma filial remota com um link fraco. Isso significa que o Agente ERA em cada cliente não está conectando ao Servidor ERA principal diretamente através do Proxy ERA, que está na mesma rede local da filial. Esta configuração libera o link da filial. O Proxy ERA aceita conexões de todos os Agentes ERA locais, compila seus dados e os envia para o Servidor ERA principal (ou outro Proxy ERA). Isso permite que sua rede acomode mais clientes sem comprometer o desempenho de suas consultas de banco de dados e rede.

Dependendo da configuração de sua rede, é possível que um Proxy ERA se conecte a outro Proxy ERA e então se conecte ao Servidor ERA principal.

Para o funcionamento correto do Proxy ERA, o computador host no qual você instalará o Proxy ERA deverá ter um Agente da ESET instalado e deve estar conectado ao nível superior (seja Servidor ERA ou Proxy ERA superior, se houver um) de sua rede.

2.4 Agente

O **Agente ERA** é uma parte essencial do produto ESET Remote Administrator. As soluções de segurança ESET nas máquinas dos clientes (por exemplo ESET Endpoint Security) comunicam-se com o Servidor ERA exclusivamente por meio do Agente. Esta comunicação permite o gerenciamento das soluções de segurança ESET em todos os clientes remotos a partir de um local central. O Agente coleta informações do cliente e as envia para o Servidor. Quando o Servidor envia uma tarefa para o cliente, ela é enviada para o Agente, que então comunica-se com o cliente. Toda a comunicação em rede ocorre entre o Agente e a parte superior da rede do ERA: Servidor e Proxy.

O Agente ESET usa um dos seguintes três métodos para se conectar ao Servidor:

1. O Agente do Cliente é diretamente conectado ao Servidor.
2. O Agente do Cliente é conectado através de um Proxy, que é conectado ao Servidor.
3. O Agente do Cliente é conectado ao Servidor através de vários Proxies.

O Agente ESET comunica-se com soluções da ESET instaladas em um cliente, coleta informações de programas nesse cliente e transmite as informações de configuração recebidas do Servidor para o cliente.

OBSERVAÇÃO: o proxy da ESET tem seu próprio Agente, que processa todas as tarefas de comunicação entre clientes, outros proxies e o Servidor.

2.5 RD Sensor

Sensor RD (Rogue Detection) é parte do ESET Remote Administrator desenvolvido para encontrar computadores na sua rede. Ele oferece uma forma conveniente de adicionar novos computadores ao ESET Remote Administrator sem a necessidade de encontrá-los e adicioná-los manualmente. Todo computador detectado em sua rede é exibido no console da Web e é adicionado por padrão ao grupo **Todos**. A partir daí, é possível realizar ações adicionais com computadores cliente individuais.

O RD Sensor consiste em um mecanismo de escuta passivo que detecta computadores que estão presentes na rede e envia informações sobre eles para o Servidor ERA. O Servidor ERA avalia se os PCs detectados na rede são desconhecidos ou se já são gerenciados.

3. Usando o ESET Endpoint Security sozinho

Esta seção do guia do usuário é feita para usuários que estão utilizando o ESET Endpoint Security sem o ESET Remote Administrator. Todos os recursos e funcionalidades do ESET Endpoint Security estão totalmente acessíveis dependendo dos registros da conta do usuário.

3.1 Instalação com o ESET AV Remover

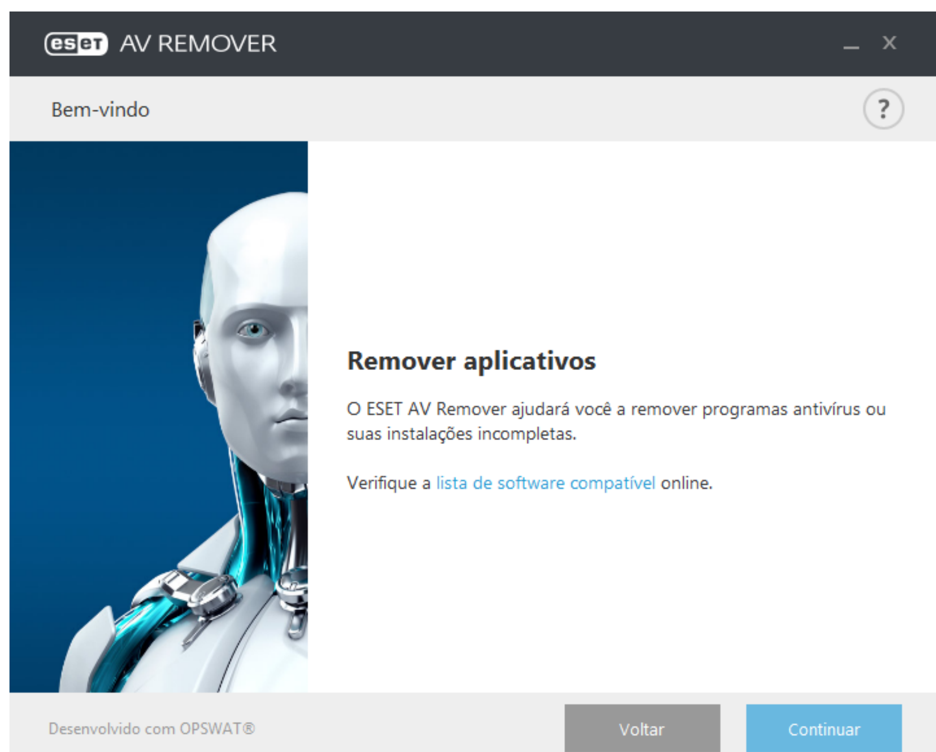
Antes de continuar com o processo de instalação, é importante que outros aplicativos de segurança existentes no computador sejam desinstalados. Selecione a caixa de seleção ao lado de **Quero desinstalar aplicativos antivírus indesejados usando o ESET AV Remover** para que o ESET AV Remover rastreie seu sistema e remova qualquer aplicativo de segurança compatível. Deixe a guia caixa de seleção desmarcada e clique em **Continuar** para instalar o ESET Endpoint Security sem executar o ESET AV Remover.



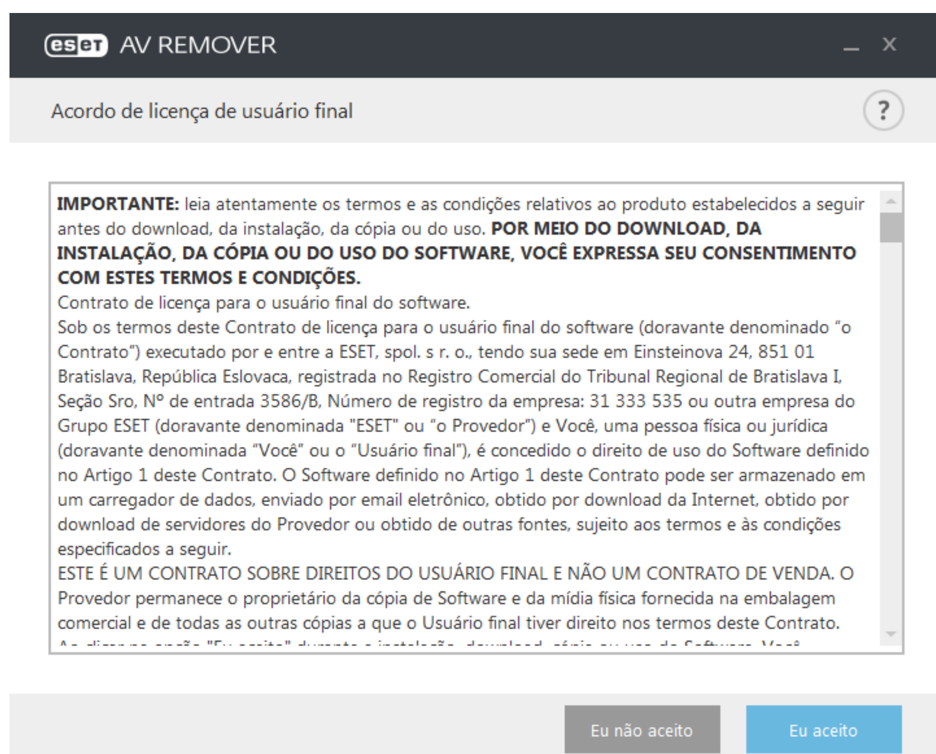
3.1.1 ESET AV Remover

A ferramenta ESET AV Remover ajudará você a remover quase todos os software antivírus instalados anteriormente no seu sistema. Siga as instruções abaixo para remover um programa antivírus existente usando o ESET AV Remover:

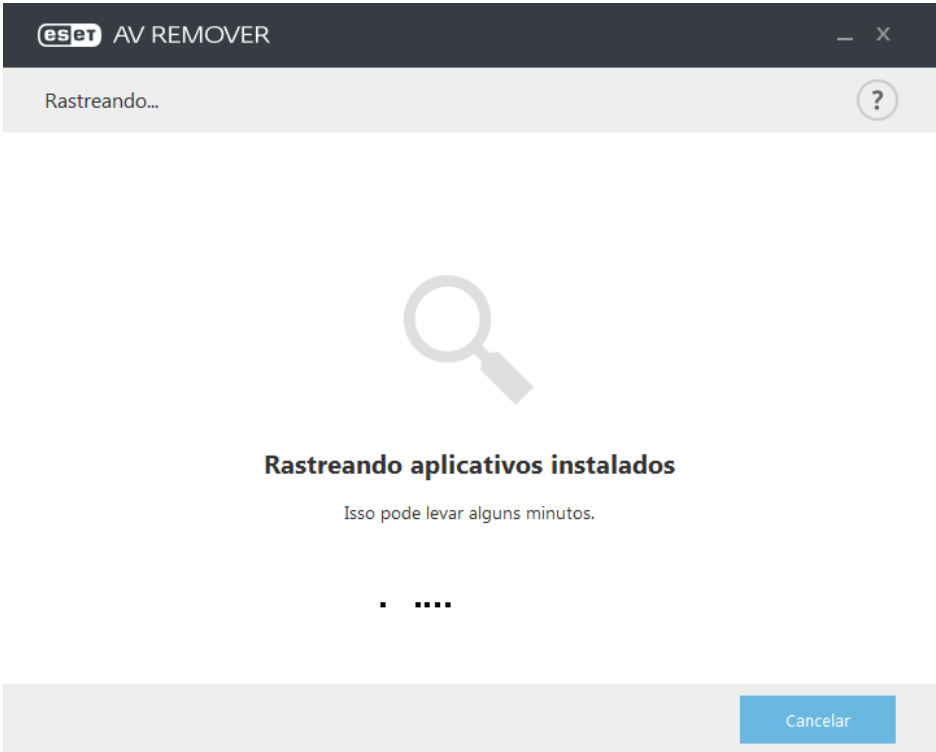
1. Para ver uma lista de software antivírus que o ESET AV Remover pode remover, visite o Artigo na base de conhecimento ESET.



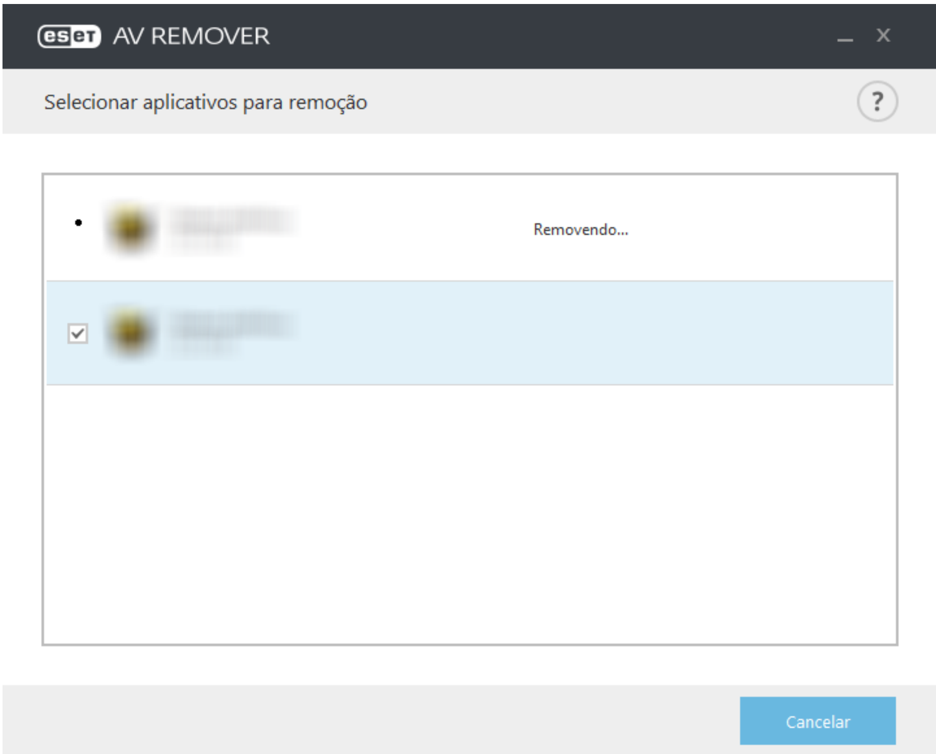
2. Leia-o e clique em **Aceitar** para confirmar a sua aceitação do Contrato de licença de usuário final. Clicar em **Eu não aceito** vai continuar com a instalação do ESET Endpoint Security sem remover qualquer aplicativo de segurança existente no computador.



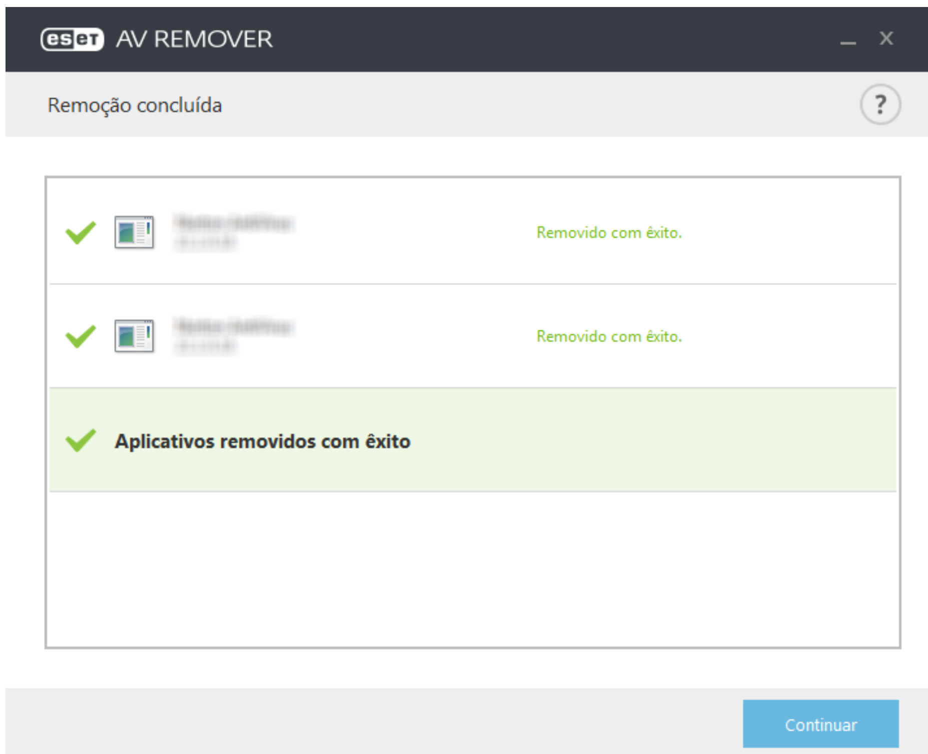
3. o ESET AV Remover começará a procurar por software antivírus no seu sistema.



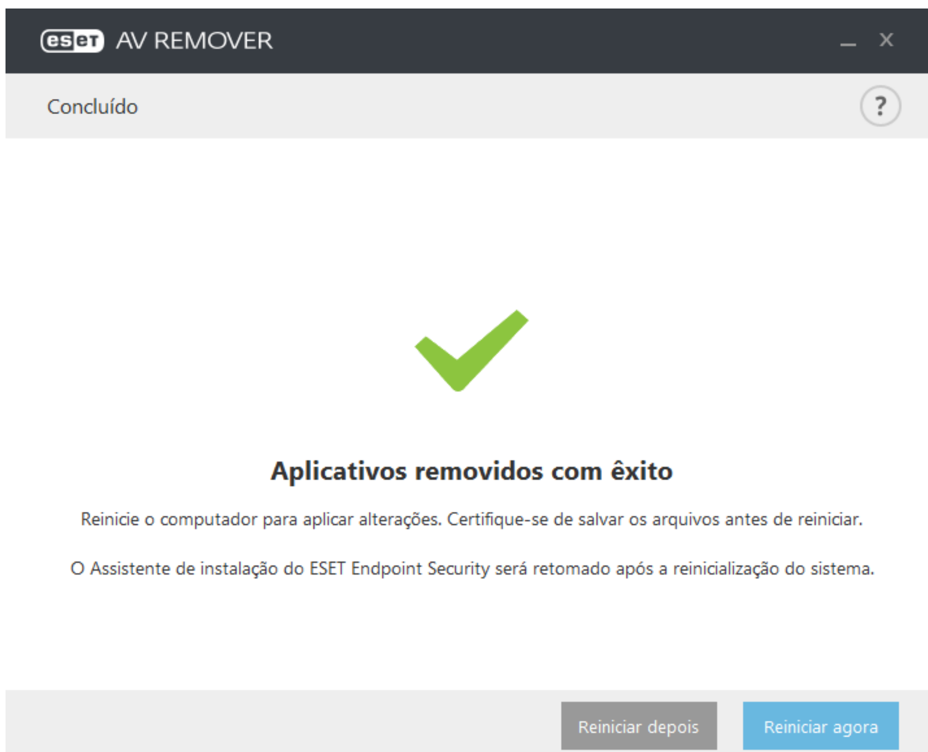
4. Selecione qualquer aplicativo antivírus listado e clique em Remover. A remoção pode levar alguns minutos.



5. Quando a remoção é bem sucedida, clique em **Continuar**.



6. Reinicie seu computador para aplicar as alterações e continue com a instalação do ESET Endpoint Security. Se a desinstalação não for bem sucedida, consulte a seção Desinstalação com o ESET AV Remover terminou com erro deste guia.



3.1.2 Desinstalação usando o ESET AV Remover terminou com erro

Se você não conseguir remover um programa antivírus usando o ESET AV Remover, você receberá uma notificação de que o aplicativo que está tentando remover pode não ser compatível com o ESET AV Remover. Visite a lista de produtos compatíveis ou desinstaladores para software antivírus comuns do Windows na Base de conhecimento ESET para ver se este programa específico pode ser removido.

Quando a desinstalação do produto de segurança não foi bem sucedida ou parte do seu componente foi desinstalado parcialmente, você é solicitado a **Reiniciar e rastrear novamente**. Confirmar UAC depois da inicialização e continuar com o processo de rastreamento e desinstalação.

Se necessário, entre em contato com o Atendimento ao cliente ESET para abrir uma solicitação de suporte e para que o arquivo **AppRemover.log** esteja disponível para ajudar os técnicos da ESET. O arquivo **AppRemover.log** está localizado na pasta **eset**. Procure o *%TEMP%* no Windows Explorer para acessar esta pasta. O Atendimento ao Cliente da ESET responderá o mais rápido possível para ajudar a resolver seu problema.

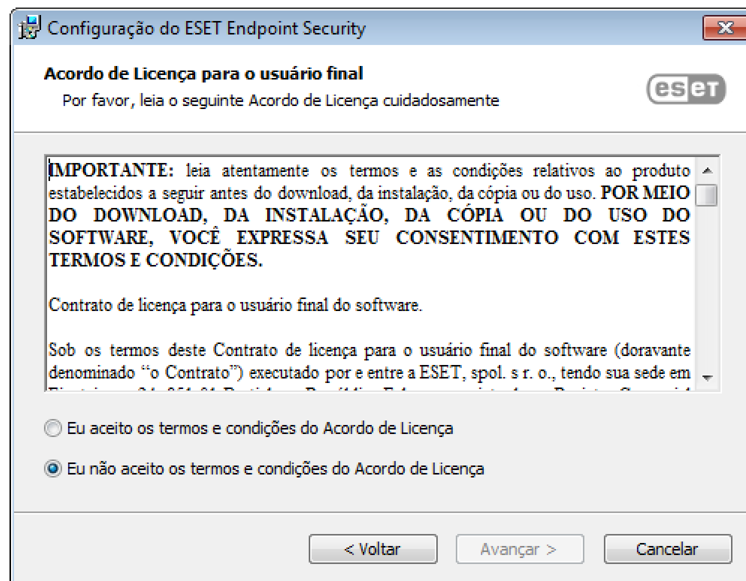
3.2 Instalação

Inicie o instalador e o assistente de instalação o guiará pelo processo de instalação.

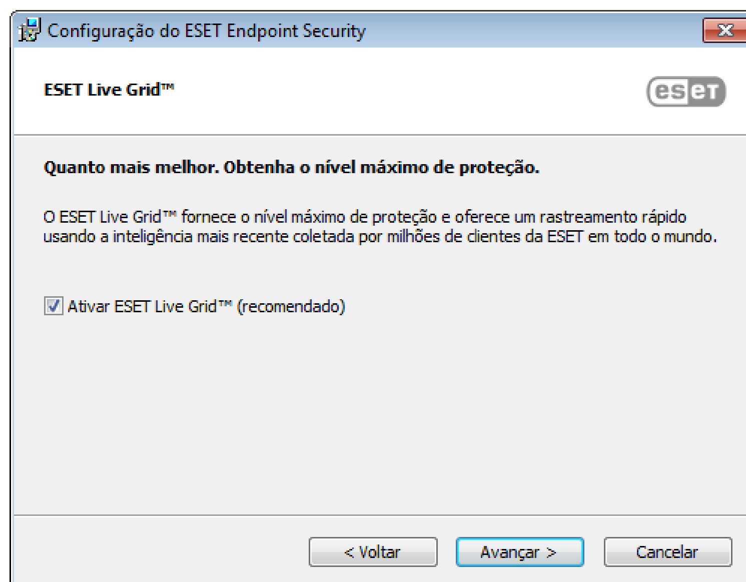
Importante: Verifique se não há algum outro programa antivírus instalado no computador. Se duas ou mais soluções antivírus estiverem instaladas em um único computador, elas podem entrar em conflito umas com as outras. Recomendamos desinstalar outros programas antivírus do sistema. Consulte nosso artigo da base de conhecimento para obter uma lista de ferramentas de desinstalação para os softwares de antivírus comuns (disponível em inglês e vários outros idiomas).



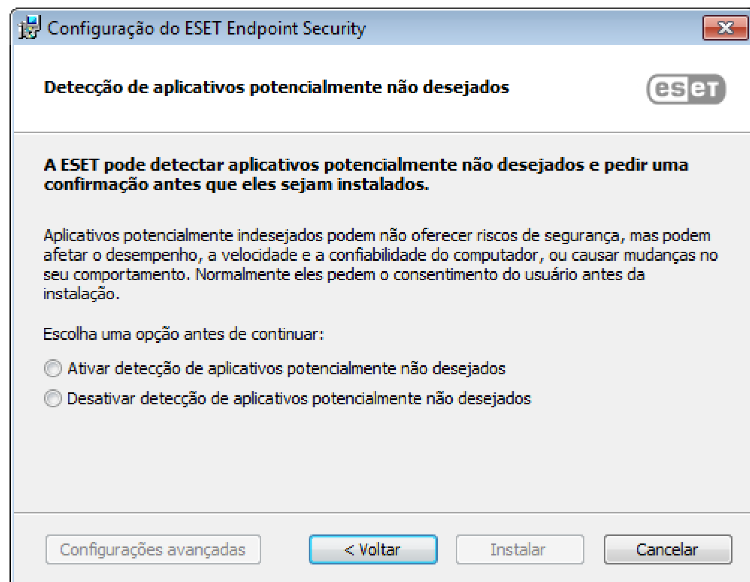
Na próxima etapa, o Contrato de licença de usuário final será exibido. Leia-o e clique em **Aceitar** para confirmar a sua aceitação do Contrato de licença de usuário final. Clique em **Avançar** depois de aceitar os termos para continuar com a instalação.



Depois de selecionar "Aceitar..." e clicar em **Avançar**, será solicitado que você configure o ESET Live Grid. O ESET Live Grid ajuda a assegurar que a ESET seja informada contínua e imediatamente sobre novas infiltrações para proteger seus clientes. O sistema permite o envio de novas ameaças para o Laboratório de vírus da ESET, onde elas são analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus.



A próxima etapa no processo de instalação é configurar a detecção de aplicativos potencialmente indesejados que não são necessariamente maliciosos, mas com frequência afetam negativamente o comportamento de seu sistema operacional. Consulte o capítulo Aplicativos potencialmente indesejados para obter mais detalhes. Você pode acessar configurações adicionais clicando em **Configurações avançadas** (por exemplo, para instalar seu produto ESET em uma pasta específica ou ativar o rastreamento automático após a instalação).



A etapa final é confirmar a instalação clicando em **Instalar**.

3.2.1 Instalação avançada

A instalação avançada permitirá que você personalize vários parâmetros de instalação não disponíveis ao realizar uma instalação típica.

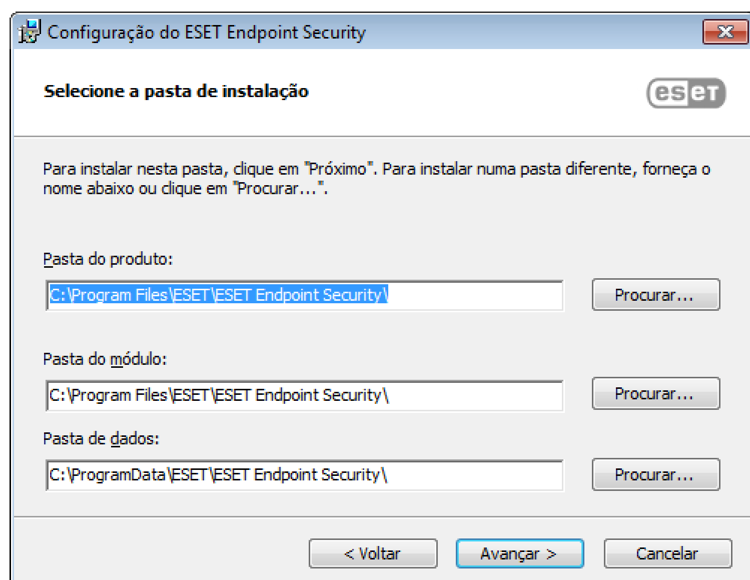
Depois de selecionar sua preferência para detecção de aplicativos potencialmente não desejados e clicar em **Configurações avançadas**, você será solicitado a selecionar um local para a pasta do produto de instalação. Por padrão, o programa é instalado no seguinte diretório:

C:\Program Files\ESET\ESET Endpoint Security

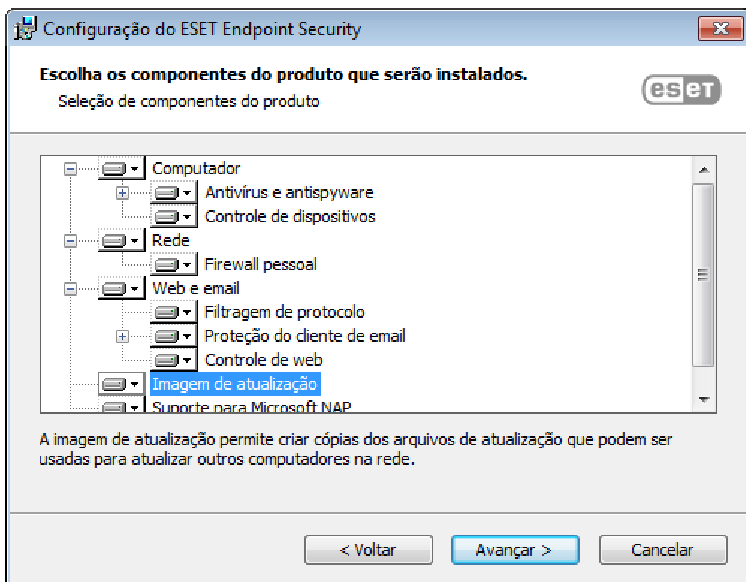
Você pode especificar um local para dados e módulos de programa. Por padrão, eles são instalados nos seguintes diretórios:

C:\Program Files\ESET\ESET Endpoint Security
C:\ProgramData\ESET\ESET Endpoint Security

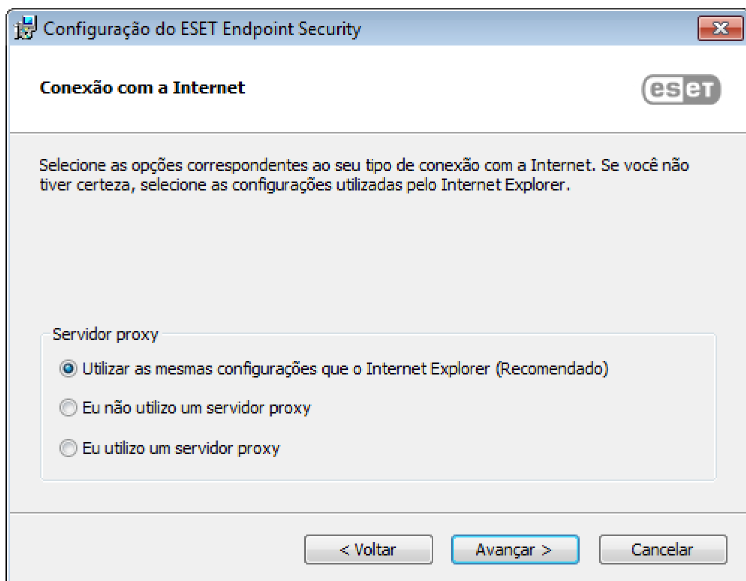
Clique em **Procurar...** para alterar esses locais (não recomendado).



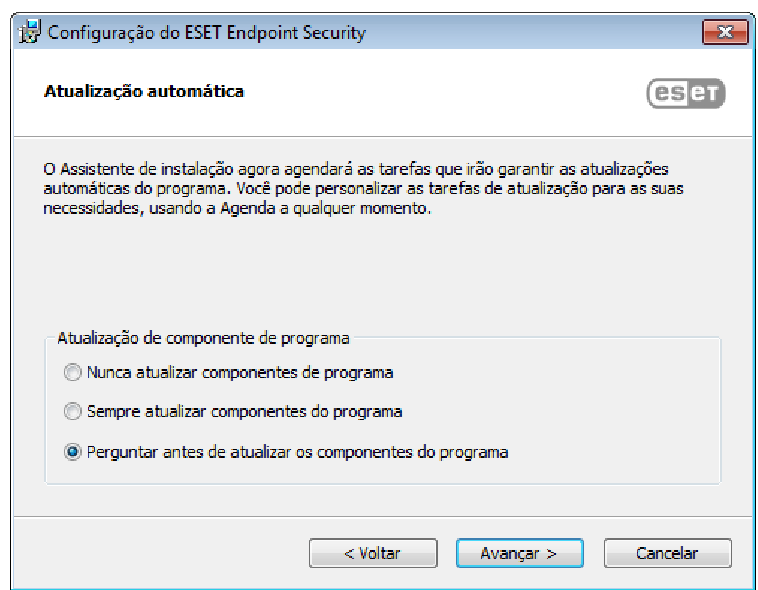
Na próxima janela, você pode escolher quais componentes de produto serão instalados. Os componentes do programa na seção Computador representam a Proteção em tempo real do sistema de arquivos, Rastreamento do computador, Proteção de documentos e Controle de dispositivos. Observe que os dois primeiros componentes são obrigatórios para que a sua solução de segurança funcione. A seção Rede oferece a opção de instalação do Firewall pessoal, que monitora todo o tráfego de entrada e saída na rede, e aplica regras para conexões individuais de rede. O Firewall pessoal também fornece proteção contra ataques de computadores remotos. Os componentes na seção Web e email são responsáveis pela sua proteção ao navegar na Internet e comunicar-se via email. O componente Mirror de atualização pode ser usado para atualizar outros componentes em sua rede. A seção Proteção do acesso à rede (NAP) da Microsoft fornece um agente da ESET para garantir total compatibilidade com a arquitetura da NAP.



Para definir as configurações do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Próximo**. Digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. Se você não tiver certeza se deve usar um servidor proxy para se conectar à Internet, selecione **Utilizar as mesmas configurações que o Internet Explorer (Recomendado)** e clique em **Próximo**. Se você não utilizar um servidor proxy, selecione **Eu não utilizo um servidor proxy**. Para obter mais informações, consulte Servidor proxy.

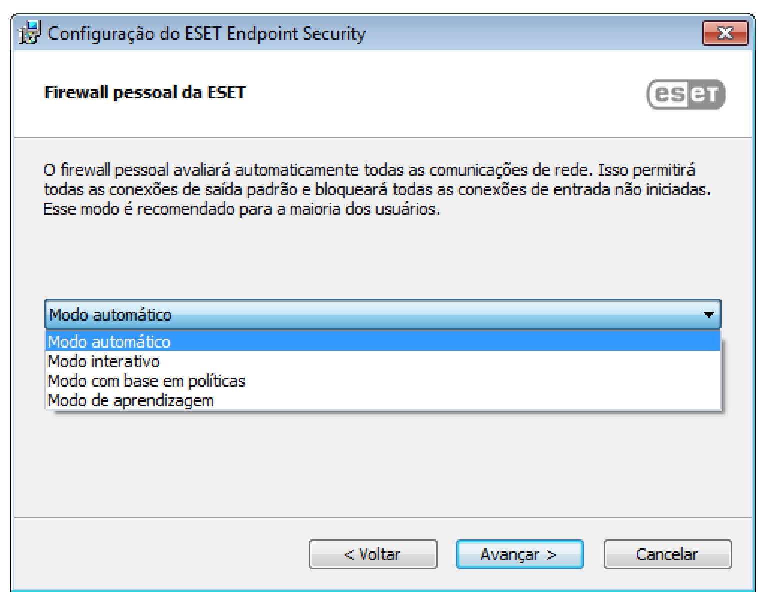


A instalação personalizada permite definir como as atualizações automáticas do programa serão tratadas no sistema. Clique em **Alterar...** para acessar as Configurações avançadas.



Se não desejar atualizar os componentes do programa, selecione **Nunca atualizar componentes de programa**. Selecione **Perguntar antes de fazer download dos componentes de programa** para exibir uma janela de confirmação sempre que o sistema tentar fazer download dos componentes de programa. Para fazer download automaticamente de atualizações dos componentes do programa, selecione a opção **Sempre atualizar componentes do programa**.

Em seguida, selecione um modo de filtragem para o firewall pessoal da ESET. Quatro modos de filtragem estão disponíveis para o firewall pessoal do ESET Endpoint Security. O comportamento do firewall é alterado com base no modo selecionado. Os modos de filtragem também influenciam o nível de interação necessário do usuário.



A próxima janela da instalação oferecerá a opção de definir uma senha para proteger as configurações do programa. Selecione **Proteger as configurações por senha** e digite a sua senha nos campos **Nova senha** e **Confirmar nova senha**. Esta senha será solicitada em todas modificações ou acessos futuros no ESET Endpoint Security. Quando ambos os campos de senha coincidirem, clique em **Próximo** para continuar.

Configuração do ESET Endpoint Security
Configurações protegidas por senha
Proteger as configurações por senha
Nova senha:
Confirmar nova senha:
< Voltar Avançar > Cancelar

Para desativar o primeiro rastreamento após a instalação que normalmente é realizado quando a instalação termina, desmarque a caixa de seleção ao lado de **Ativar o rastreamento após a instalação**.

Configuração do ESET Endpoint Security
Rastreamento automático depois da instalação
Ativar o rastreamento automático depois da instalação para verificar a existência de malware e melhorar o desempenho futuro de rastreamento.
Ativar rastreamento depois da instalação
< Voltar Instalar Cancelar

Clique em **Instalar** para iniciar a instalação.

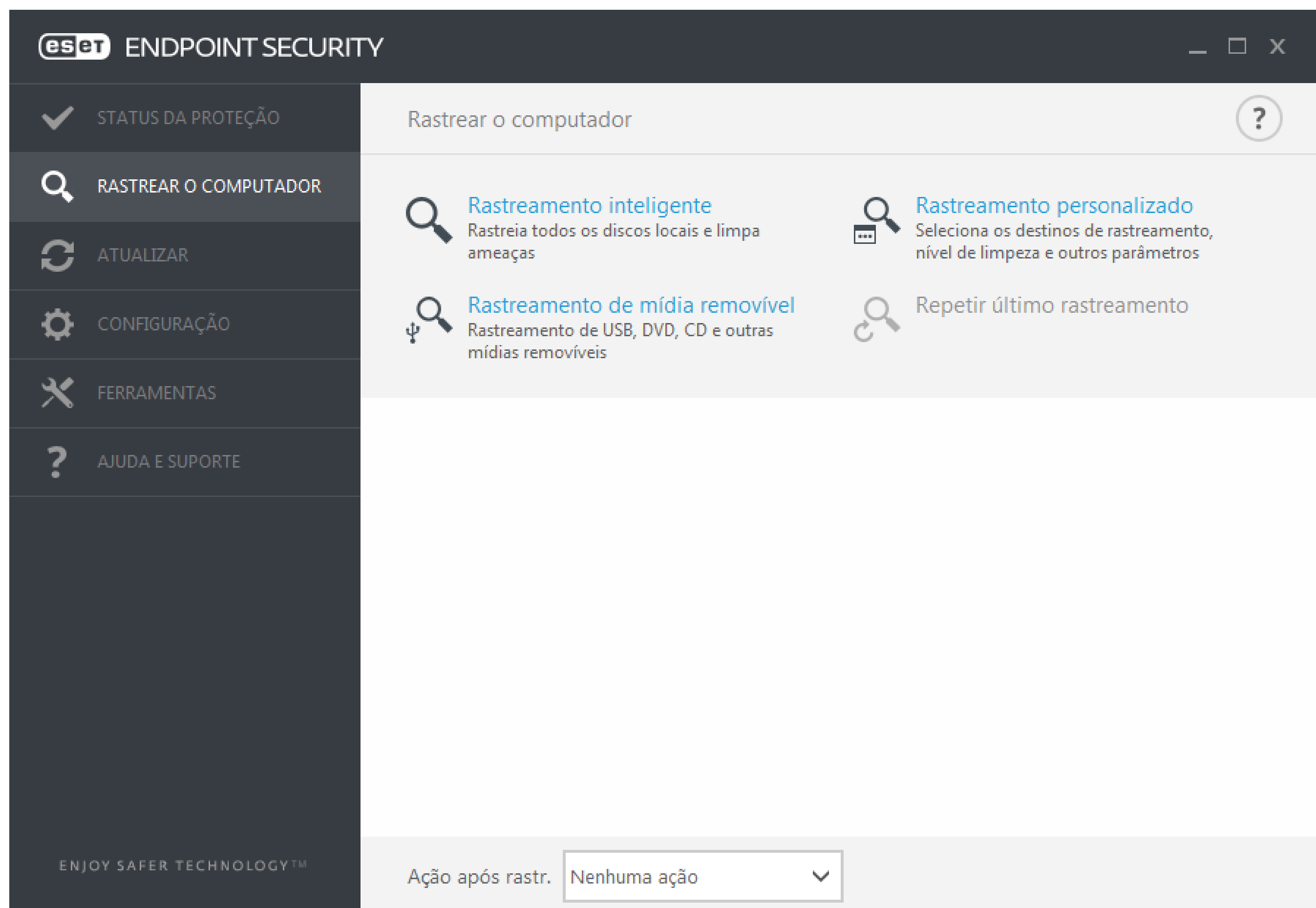
3.3 Ativação do produto

Após a conclusão da instalação, você será solicitado a ativar o produto.

Selecione um dos métodos disponíveis para ativar o ESET Endpoint Security. Para obter mais informações, consulte Como ativar o ESET Endpoint Security.

3.4 Rastrear o computador

No máximo 15 minutos depois da conclusão da instalação (pode ser necessário reiniciar o computador), o ESET Endpoint Security realizará automaticamente um rastreamento do computador. Além do rastreamento inicial, recomendamos que você realize rastreamentos regulares do computador ou agende um rastreamento regular para verificar se há ameaças. Na janela principal do programa, clique em **Rastrear o computador** e, em seguida, clique em **Rastreamento inteligente**. Para obter mais informações sobre rastreamentos do computador, consulte Rastrear o computador.



3.5 Atualização para uma versão mais recente

Versões mais recentes do ESET Endpoint Security são lançadas para fornecer aprimoramentos ou corrigir problemas que não podem ser resolvidos por meio de atualizações automáticas dos módulos do programa. A atualização para uma versão mais recente pode ser feita de várias formas:

1. Automaticamente, por meio de uma atualização do programa.
   Como a atualização do programa é distribuída para todos os usuários e pode ter impacto em determinadas configurações do sistema, ela é lançada depois de um longo período de testes para funcionar com todas as configurações de sistema possíveis. Se você precisar atualizar para uma versão mais recente imediatamente após ela ter sido lançada, use um dos métodos a seguir.
2. Manualmente, por meio de download e instalação de uma versão mais recente sobre a instalação anterior.
3. Manualmente, através da implementação automática em um ambiente de rede usando o ESET Remote Administrator.

3.6 Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET Endpoint Security e de suas configurações básicas.

3.6.1 A interface do usuário

A janela principal do ESET Endpoint Security é dividida em duas seções principais. A primeira janela à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

Status da proteção - Fornece informações sobre o status da proteção do ESET Endpoint Security.

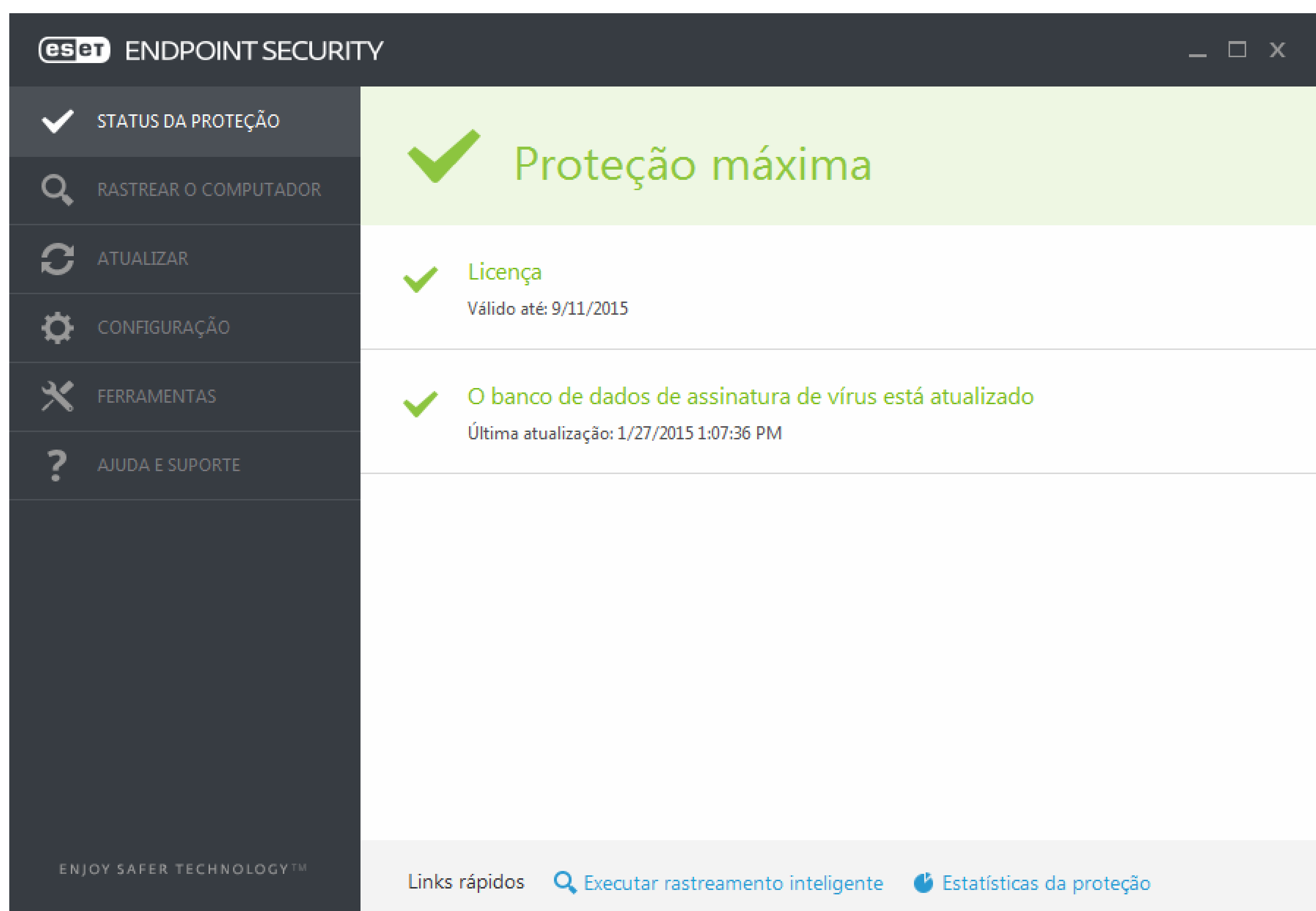
Rastrear o computador - Essa opção permite que você configure e inicie o Rastreamento inteligente, o Rastreamento personalizado ou Rastreamento de mídia removível. Você também pode repetir o último rastreamento que foi executado.

Atualizar - Exibe informações sobre o banco de dados de assinatura de vírus.

Configuração - Selecione essa opção para ajustar configurações de segurança de seu Computador, Rede ou Web e Email.

Ferramentas - Fornece acesso a arquivos de log, estatísticas de proteção, monitoramento de atividade, processos em execução, Agendador, Quarentena, conexões de rede, ESET SysInspector e ESET SysRescue para criar um CD de restauração. Você também pode enviar uma amostra para análise.

Ajuda e suporte - Fornece acesso a arquivos de ajuda, base de conhecimento da ESET e site da empresa ESET. Além disso, estão disponíveis links para abrir uma solicitação de suporte do Atendimento ao cliente, ferramentas de suporte e informações sobre ativação do produto.

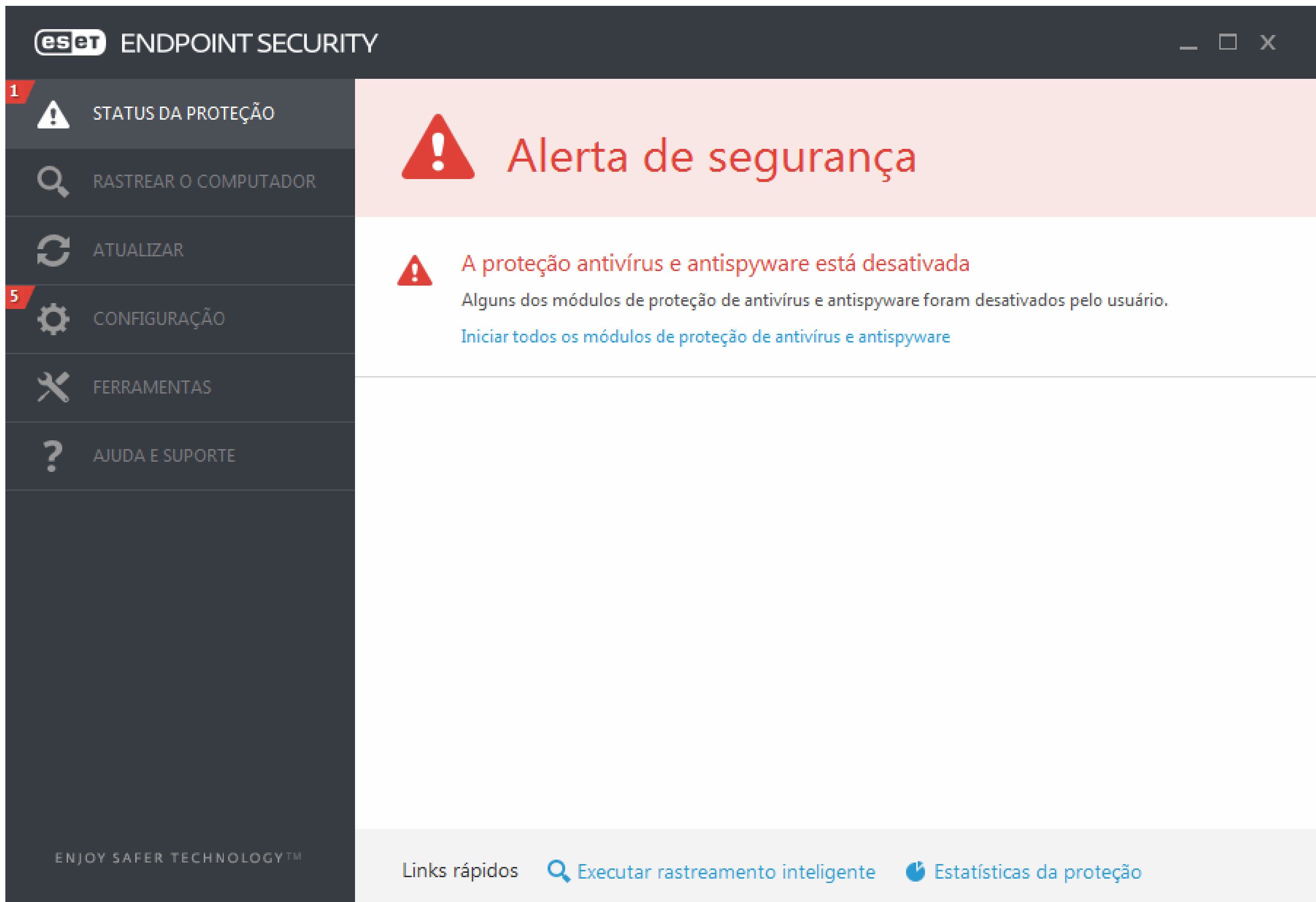


A tela **Status da proteção** informa sobre a segurança e o nível de proteção atual do seu computador. O ícone verde de status de **Proteção máxima** indica que a proteção máxima está garantida.

A janela de status também exibe os links rápidos para recursos mais usados do ESET Endpoint Security e informações sobre a última atualização.

O que fazer se o programa não funcionar adequadamente?

Se os módulos ativados estiverem funcionando adequadamente, um ícone de marcação verde será atribuído a eles. Caso contrário, um ponto de exclamação vermelho ou um ícone de notificação laranja será exibido. Informações adicionais sobre o módulo serão mostradas na parte superior da janela. Uma solução sugerida para corrigir o módulo também é exibida. Para alterar o status de módulos individuais, clique em **Configuração** no menu principal e clique no módulo desejado.



O ícone vermelho com um "!" assinala problemas críticos - a proteção máxima do seu computador não está garantida. As possíveis razões são:

- **Proteção antivírus e antispyware desativada** - Você pode reativar a proteção antivírus e antispyware clicando em **Ativar proteção em tempo real** no painel **Status da proteção** ou no painel **Ativar proteção antivírus e antispyware** no painel **Configuração** na janela principal do programa.
- **O firewall pessoal do ESET está desativado** - Esse problema é indicado por um ícone vermelho e uma notificação de segurança próxima ao item **Rede**. Você pode reativar a proteção da rede clicando em **Ativar modo de filtragem**.
- **Banco de dados de assinatura de vírus desatualizado** - Você está usando um banco de dados de assinatura de vírus desatualizado.
- **Produto não ativado** ou **Licença expirada** - Isso é indicado pelo ícone do status de proteção que fica vermelho. O programa não pode ser atualizado após a licença expirar. Recomendamos que você siga as instruções da janela de alerta para renovar sua licença.

O ícone laranja com um "i" indica que seu produto ESET requer atenção devido a um problema não crítico. As possíveis razões são:

- **A proteção do acesso à web está desativada** - Você pode reativar a proteção do acesso à web clicando na notificação de segurança e em **Ativar proteção do acesso à web**.

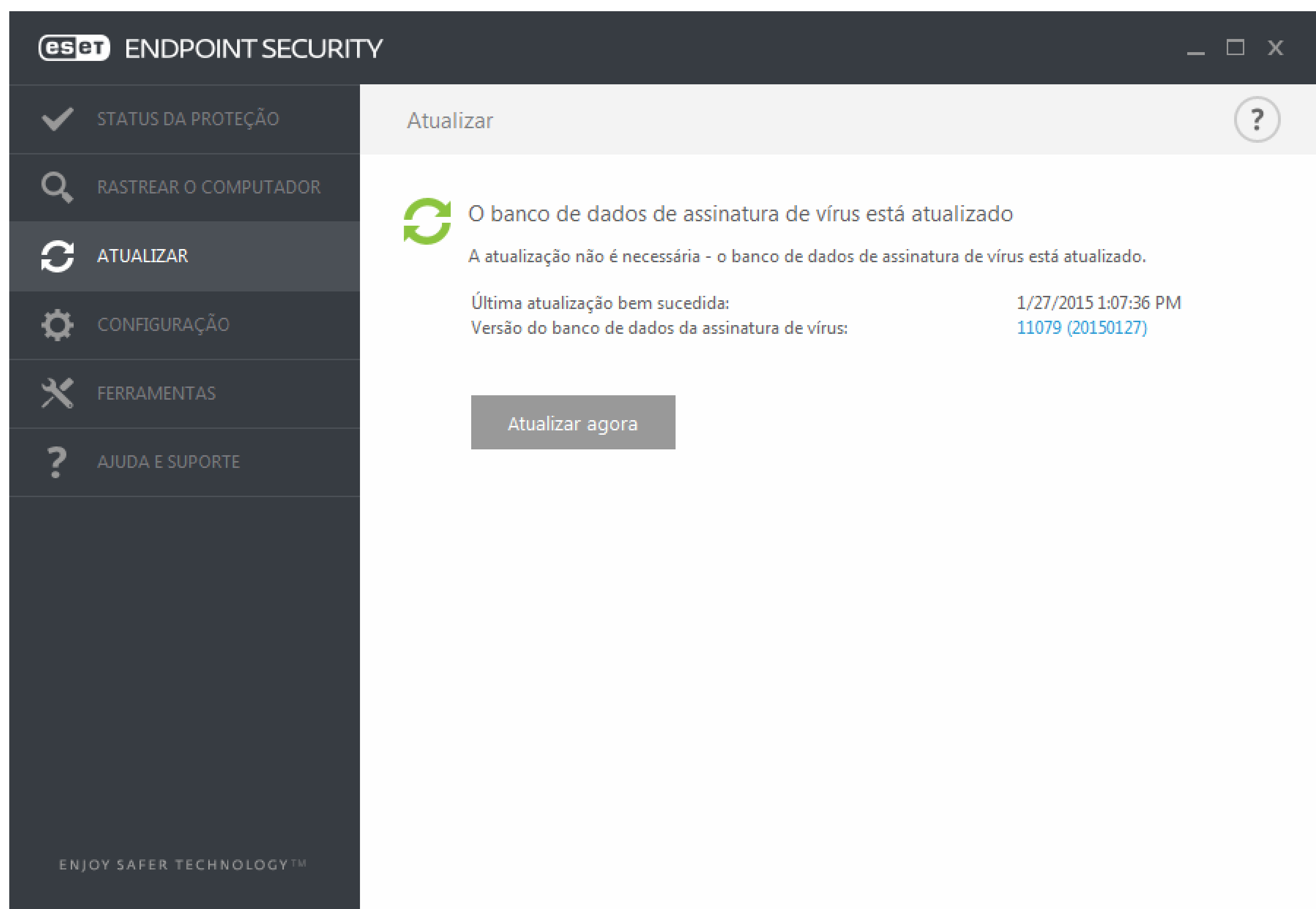
- **Sua licença expirará em breve** - Isso é indicado pelo ícone do status de proteção exibindo um ponto de exclamação. Depois que a licença expirar, o programa não poderá ser atualizado e o ícone do status da proteção ficará vermelho.

Se não for possível solucionar um problema com as soluções sugeridas, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou pesquisar na Base de conhecimento da ESET. Se precisar de assistência, entre em contato com o Atendimento ao Cliente da ESET. O Atendimento ao Cliente da ESET responderá rapidamente às suas dúvidas e o ajudará a encontrar uma solução.

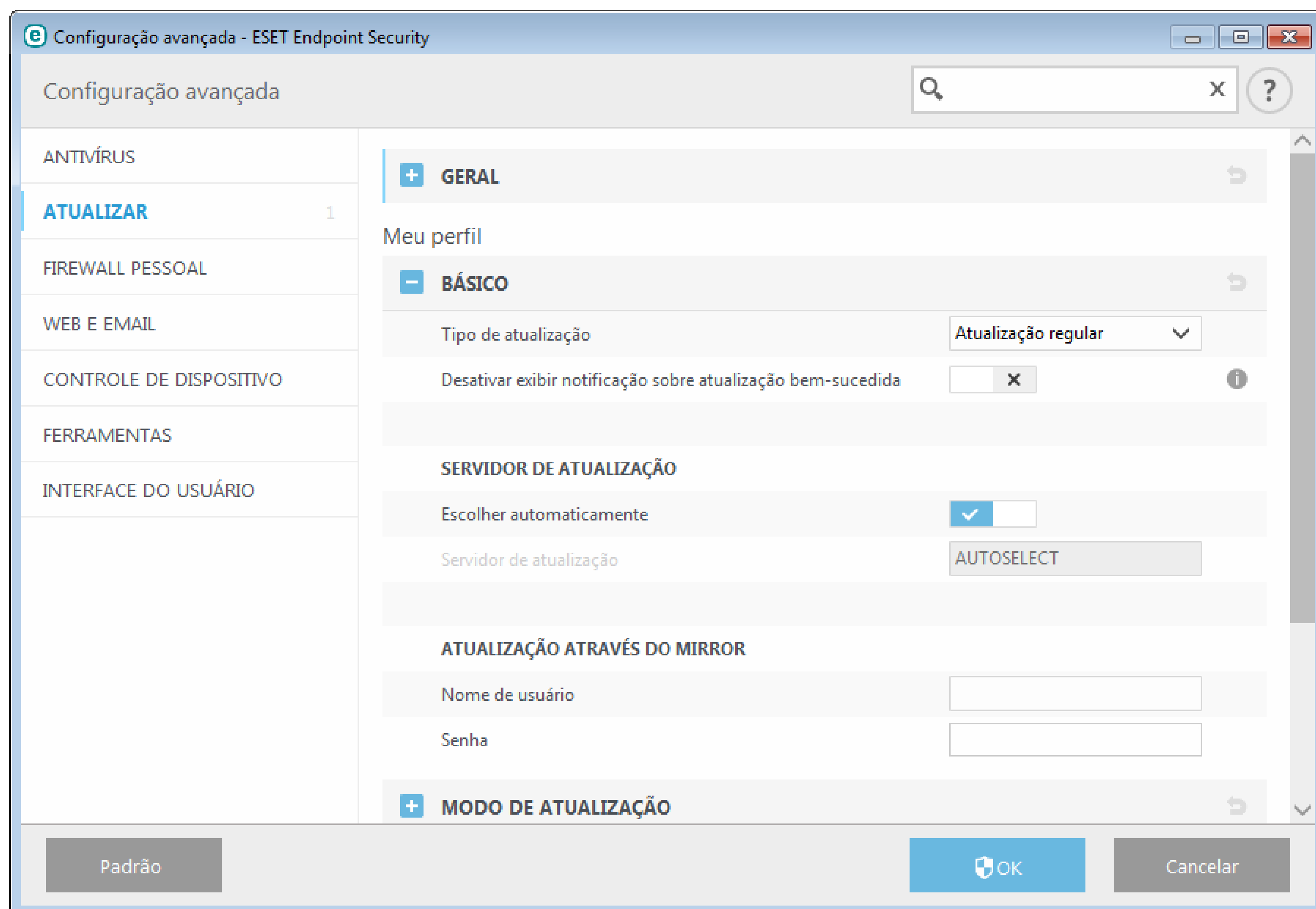
3.6.2 Configuração da atualização

A atualização do banco de dados de assinatura de vírus e dos componentes do programa é uma parte importante para manter a proteção completa contra códigos maliciosos. Preste bastante atenção na configuração de atualização e operação. No menu principal, selecione **Atualizar** > **Atualizar agora** para verificar se há uma atualização mais recente do banco de dados.

Se a sua **Chave de licença** ainda não foi inserida, não será possível receber novas atualizações e você será solicitado a ativar seu produto.



A janela Configuração avançada (no menu principal, clique em **Configuração** > **Configuração avançada**, ou pressione **F5** no teclado) contém opções de atualização adicionais. Para configurar as opções avançadas de atualização, como o modo de atualização, o acesso ao servidor proxy, as conexões de rede e as configurações de criação de cópias do banco de dados de assinatura de vírus, clique em **Atualizar** na árvore Configuração avançada. Se tiver problemas com uma atualização, clique em **Limpar** para limpar o cache de atualização temporário. Por padrão, o menu **Servidor de atualização** está definido como **SELEÇÃO AUTOMÁTICA**. Ao usar um servidor ESET, recomendamos que você deixe a opção **Escolher automaticamente** selecionada. Se você não quiser que a notificação da bandeja do sistema no canto inferior direito da tela seja exibida, selecione **Desativar exibir notificação sobre atualização bem-sucedida**.



Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Essa ação somente será possível se a **Chave de licença** correta for inserida em **Ajuda e suporte** > **Ativar produto**.

Se você não inseriu sua **chave de licença** após a instalação, poderá inseri-la a qualquer momento. Para obter informações mais detalhadas sobre a ativação, consulte Como ativar o ESET Endpoint Security e insira as credenciais recebidas com o produto de segurança ESET na janela **Detalhes da licença**.

3.6.3 Configuração de zonas

É necessário configurar zonas confiáveis para proteger o computador em um ambiente de rede. É possível permitir que outros usuários acessem o seu computador configurando a zona confiável e permitindo o compartilhamento. Clique em **Configuração avançada** (F5) > **Firewall pessoal** > **Zonas** para acessar configurações de zonas confiáveis.

A detecção de zona confiável ocorre após a instalação do ESET Endpoint Security e sempre que o seu computador se conectar a uma nova rede, portanto, na maioria dos casos não há necessidade de definir a zona confiável. Por padrão, há uma janela da caixa de diálogo exibida na detecção de uma nova zona que permite configurar o nível de proteção dessa zona.



Aviso: Uma configuração incorreta da zona confiável pode representar um risco de segurança para o seu computador.

OBSERVAÇÃO: Por padrão, as estações de trabalho de uma Zona confiável têm acesso garantido a arquivos e impressoras compartilhados, a comunicação RPC de entrada é ativada e o compartilhamento da área de trabalho remota é disponibilizado.

3.6.4 Ferramentas de controle da Web

Se você já tiver ativado o Controle de web no ESET Endpoint Security, também deverá configurar o Controle de web para contas de usuário desejadas, a fim de que o Controle de web funcione devidamente. Consulte o capítulo Controle de web para obter instruções sobre como criar restrições específicas para suas estações de trabalho clientes, a fim de protegê-los de material potencialmente ofensivo.

3.7 Dúvidas comuns

Este capítulo contém algumas perguntas e problemas mais freqüentes encontrados. Clique em um título do capítulo para descobrir como solucionar o seu problema:

Como atualizar o ESET Endpoint Security
Como ativar o ESET Endpoint Security
Como usar credenciais atuais para ativar um novo produto
Como remover um vírus do meu PC
Como permitir comunicação para um determinado aplicativo
Como criar uma nova tarefa na Agenda
Como agendar uma tarefa de rastreamento (a cada 24 horas)
Como conectar meu produto ao ESET Remote Administrator
Como configurar uma imagem

Se o seu problema não estiver incluído na lista das páginas de ajuda acima, tente pesquisar por palavra-chave ou digite uma frase descrevendo seu problema nas páginas de ajuda do ESET Endpoint Security.

Se não conseguir encontrar a solução para o seu problema/pergunta dentro das páginas de Ajuda, poderá acessar nossa Base de conhecimento ESET onde estão disponíveis respostas para perguntas e problemas comuns.

Como removo o cavalo de troia Sirefef (ZeroAccess)?
Lista de verificação de solução de problemas de atualização através de imagem
Quais endereços e portas em meu firewall de terceiros devo abrir para permitir a funcionalidade total para meu produto ESET?

Se necessário, você pode contatar nosso centro de suporte técnico on-line com as suas perguntas ou problemas. O link para nosso formulário de contato on-line pode ser encontrado no painel **Ajuda e Suporte** na janela do programa principal.

3.7.1 Como atualizar o ESET Endpoint Security

A atualização do ESET Endpoint Security pode ser executada de forma manual ou automática. Para acionar a atualização, clique em **Atualizar agora** na seção **Atualização** no menu principal.

A instalação padrão cria uma tarefa de atualização automática que é executada a cada hora. Para alterar o intervalo, vá para **Ferramentas** > **Agenda** (para mais informações sobre a Agenda, clique aqui).

3.7.2 Como ativar o ESET Endpoint Security

Após a conclusão da instalação, você será solicitado a ativar o produto.

Há vários métodos para ativar seu produto. A disponibilidade de um cenário específico de ativação na janela de ativação pode variar conforme o país, assim como os meios de distribuição (CD/DVD, página da web da ESET etc.).

Para ativar sua cópia do ESET Endpoint Security diretamente do programa, clique no ícone da bandeja do sistema e selecione **Ativar licença do produto** no menu. Também é possível ativar seu produto no menu principal em **Ajuda e suporte** > **Ativar produto** ou **Status da proteção** > **Ativar produto**.

Você pode usar qualquer um dos seguintes métodos para ativar o ESET Endpoint Security:

- **Chave de licença** - Uma sequência exclusiva no formato XXXX-XXXX-XXXX-XXXX-XXXX, que é usado para identificação do proprietário da licença e para ativação da licença.
- **Admin de segurança** - Uma conta criada no portal do ESET License Administrator com credenciais (endereço de email e senha). Esse método permite que você gerencie várias licenças de um local.
- **Licença offline** - Um arquivo gerado automaticamente que será transferido para o produto da ESET para fornecer informações de licença. Se uma licença permitir que você baixe um arquivo de licença off-line (.lf), esse arquivo poderá ser usado para realizar a ativação off-line. O número de licenças off-line será subtraído do número total de licenças disponíveis. Para mais detalhes sobre a geração de um arquivo off-line consulte o Guia do Usuário do ESET License Administrator.

Clique em **Ativar mais tarde** se seu computador for um membro da rede gerenciada e seu administrador for realizar a ativação remota via ESET Remote Administrator. Você também pode usar esta opção se quiser ativar este cliente em posteriormente.

Se você tem um Usuário e Senha e não sabe como ativar o ESET Endpoint Security clique em **Eu tenho um Usuário e Senha, o que faço**. Você será redirecionado ao ESET License Administrator, onde poderá converter suas credenciais para uma Chave de licença.

Você pode alterar sua licença de produto a qualquer momento. Para isso, clique em **Ajuda e suporte** > **Gerenciar licenças** na janela do programa principal. Você verá o ID público de licença usado para identificar sua licença para o Suporte ESET. O Usuário sob o qual o computador seu computador está registrado é armazenado na seção **Sobre**, que pode ser vista clicando com o botão direito do mouse no ícone da bandeja do sistema.

OBSERVAÇÃO: O ESET Remote Administrator pode ativar computadores cliente em segundo plano usando licenças disponibilizadas pelo administrador. Para instruções sobre como fazer isso, consulte o Guia do usuário do ESET Remote Administrator.

3.7.3 Como usar credenciais atuais para ativar um novo produto

Se você já tiver seu Nome de usuário e Senha e quiser receber uma Chave de licença, acesse o portal do ESET License Administrator, onde você poderá converter suas credenciais em uma nova chave de licença.

3.7.4 Como remover um vírus do meu PC

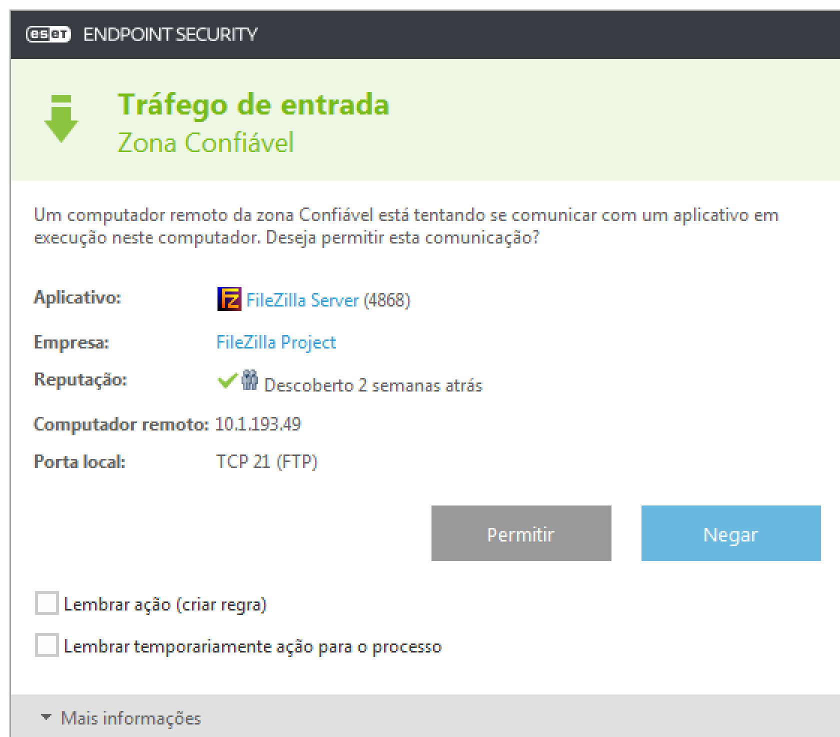
Se o seu computador estiver mostrando sintomas de uma infecção por código malicioso, como, por exemplo, estiver mais lento, congelar com frequência, recomendamos que você faça o seguinte:

1. Na janela do programa principal, clique em **Rastrear o computador**.
2. Clique em **Rastreamento inteligente** para começar o rastreamento do sistema.
3. Após a conclusão do rastreamento, revise o log com o número de arquivos verificados, infectados e limpos.
4. Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Para informações adicionais consulte nosso artigo na Base de conhecimento ESET atualizado regularmente.

3.7.5 Como permitir comunicação para um determinado aplicativo

Se uma nova conexão for detectada no modo interativo e se não houver uma regra correspondente, será solicitado que você permita ou negue a conexão. Se desejar executar a mesma ação toda vez que o ESET Endpoint Security tentar estabelecer conexão, marque a caixa de seleção **Lembrar ação (criar regra)**.



Você pode criar novas regras do firewall pessoal para aplicativos antes de eles serem detectados pelo ESET Endpoint Security na janela de configuração do firewall pessoal, localizada em **Configuração avançada** > **Firewall pessoal** > **Básico** > **Regras** clicando em **Editar**.

Clique em **Adicionar** para adicionar a regra. Na guia **Geral**, insira o nome, a direção e o protocolo de comunicação para a regra. A janela permite que você defina a ação a ser tomada quando a regra for aplicada.

Insira o caminho para o executável do aplicativo e a porta de comunicação local na guia **Local**. Clique na guia **Remoto** para inserir o endereço remoto e a porta (se aplicável). A regra recém-criada será aplicada assim que o aplicativo tentar comunicar novamente.

3.7.6 Como criar uma nova tarefa na Agenda

Para criar uma nova tarefa em **Ferramentas** > **Agenda**, clique em **Adicionar tarefa** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de logs** - Os arquivos de log também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos arquivos de log para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um snapshot do status do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Primeiro rastreamento** - por padrão, 20 minutos depois da instalação ou reinicialização um rastreamento do computador será executado como uma tarefa de baixa prioridade.
- **Atualização** - Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

Como **Atualizar** é uma das tarefas agendadas usadas com mais frequência, explicaremos a seguir como adicionar

uma nova tarefa de atualização:

No menu suspenso **Tarefa agendada**, selecione **Atualizar**. Insira o nome da tarefa no campo **Nome da tarefa** e clique em **Próximo**. Selecione a frequência da tarefa. As opções disponíveis são: **Uma vez**, **Repetidamente**, **Diariamente**, **Semanalmente** e **Acionado por evento.** Selecione **Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Depois defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As opções disponíveis são:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem **Tempo depois da última execução**)

Na próxima etapa, uma janela de resumo com informações sobre a tarefa agendada atual é exibida. Clique em **Concluir** quando tiver concluído as alterações.

Uma janela de diálogo será exibida permitindo selecionar perfis a serem utilizados para a tarefa agendada. Aqui é possível especificar um perfil primário e um alternativo, que será usado caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em **Concluir** e a nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

3.7.7 Como agendar uma tarefa de rastreamento (a cada 24 horas)

Para agendar uma tarefa regular, abra a janela do programa principal e clique em **Ferramentas** > **Agenda**. A seguir, é possível localizar uma pequena guia sobre como agendar uma tarefa. Essa tarefa criará um rastreamento nas unidades locais a cada 24 horas.

Para agendar uma tarefa de rastreamento:

1. Clique em **Adicionar** na tela principal do módulo Agenda.
2. Selecione **Rastreamento sob demanda do computador** no menu suspenso.
3. Escolha um nome para a tarefa e selecione **Repetidamente**.
4. Escolha executar a tarefa a cada 24 horas.
5. Selecione uma ação para executar se a execução da tarefa agendada falhar por algum motivo.
6. Revise o resumo da tarefa agendada e clique em **Fim**.
7. No menu suspenso **Alvos**, selecione **Unidades locais**.
8. Clique em **Concluir** para aplicar a tarefa.

3.7.8 Como conectar o ESET Endpoint Security ao ESET Remote Administrator

Quando você tiver instalado o ESET Endpoint Security em seu computador e quiser conectar-se via ESET Remote Administrator, certifique-se de que também tenha instalado o Agente ERA em sua estação de trabalho cliente. O Agente ERA é uma parte essencial de toda solução cliente que se comunica com o Servidor ERA. O ESET Remote Administrator usa a ferramenta Sensor RD para pesquisar computadores na rede. Cada computador em sua rede que for detectado pelo RD Sensor será exibido no console da web.

Assim que o Agente for implantado, você poderá realizar a instalação remota de outros produtos de segurança ESET em seus computadores cliente. As etapas exatas da instalação remota são descritas no Guia do Usuário ESET Remote Administrator.

3.7.9 Como configurar uma imagem

O ESET Endpoint Security pode ser configurado para armazenar cópias de arquivos de atualização do banco de dados de assinatura de vírus e distribuir atualizações para outras estações de trabalho com o ESET Endpoint Security ou o ESET Endpoint Antivirus em execução.

Configurando o ESET Endpoint Security como um servidor de imagem para fornecer atualizações via servidor HTTP interno

Pressione **F5** para acessar a Configuração avançada e abra **Atualizar** > **Básico**. Certifique-se de que **Servidor de atualização** está definido como **SELEÇÃO AUTOMÁTICA**. Selecione **Criar imagem da atualização** e **Fornecer arquivos de atualização através do servidor HTTP interno** de **Configuração avançada** > **Básico** > **Mirror**.

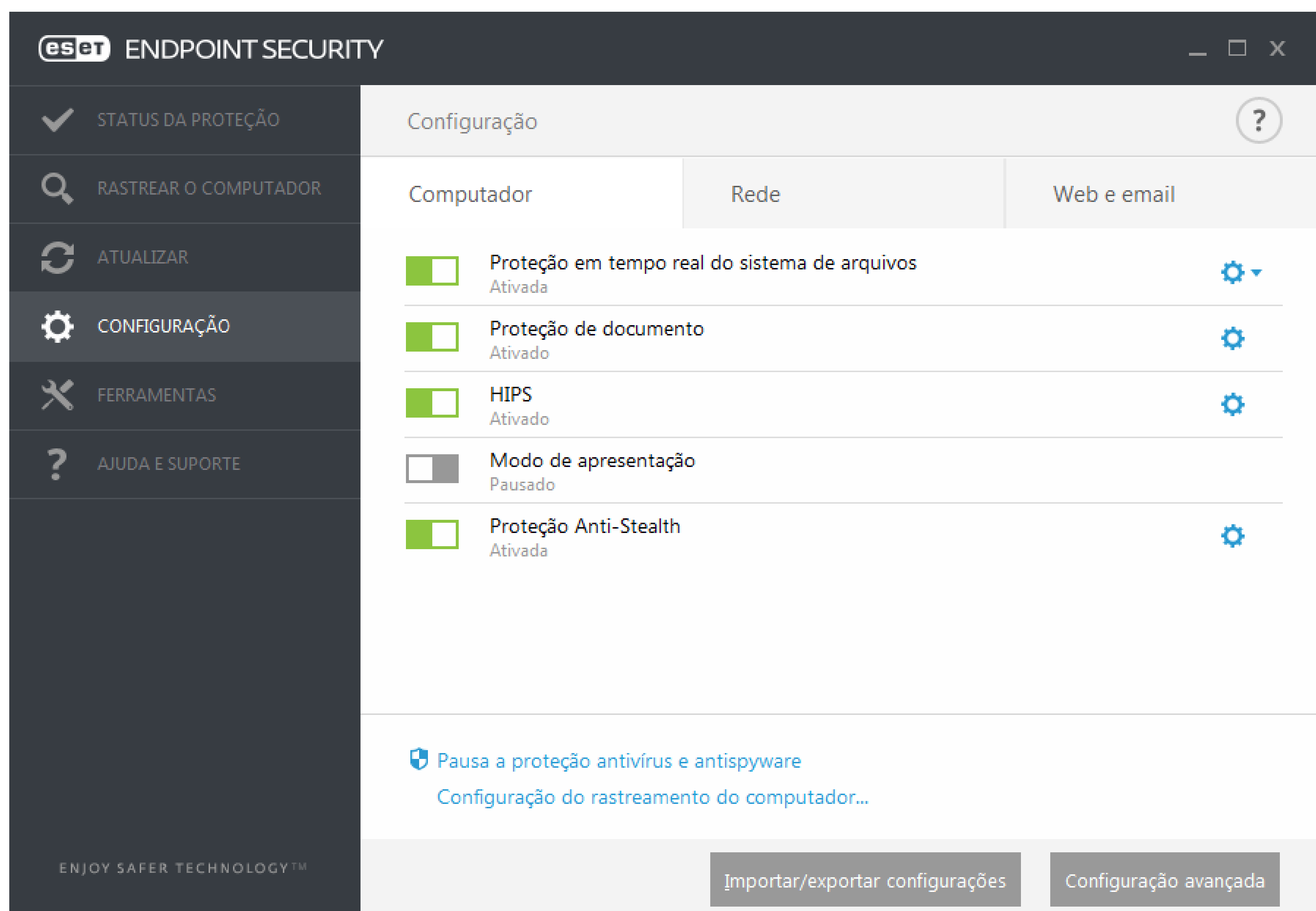
Configurando um servidor de Mirror para fornecer atualizações através de uma pasta de rede compartilhada

Crie uma pasta compartilhada em um dispositivo local ou em rede. Esta pasta deve ser lida por todos os usuários executando soluções de segurança da ESET e gravável da conta do SISTEMA local. Ative **Criar imagem da atualização** em **Configuração avançada** > **Básico** > **Imagem**. Procure e selecione a pasta compartilhada criada.

OBSERVAÇÃO: Se não quiser atualizar através do servidor interno HTTP, desative **Fornecer arquivos de atualização através do servidor HTTP**.

3.8 Trabalhar com o ESET Endpoint Security

As opções de configuração do ESET Endpoint Security permitem ajustar o nível de proteção do computador, email e rede.



O menu **Configurar** contém as seguintes seções:

- **Computador**
- **Rede**
- **Web e email**

A configuração da proteção do **Computador** permite ativar ou desativar os seguintes componentes:

- **Proteção em tempo real do sistema de arquivos** – Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador.
- **Proteção de documentos** - O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, como, por exemplo, elementos do Microsoft ActiveX.
- **HIPS** - O sistema HIPS monitora os eventos que ocorrem dentro do sistema operacional e reage a eles de acordo com um conjunto de regras personalizado.
- **Modo de apresentação** - Um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Você receberá uma mensagem de aviso (risco potencial de segurança) e a janela do programa principal será exibida em laranja após a ativação do Modo de apresentação.
- **Proteção Anti-Stealth** - Fornece a detecção de programas nocivos, como os rootkits, que podem se auto-ocultar do sistema operacional. Isso significa que não é possível detectá-los usando técnicas comuns de testes.

A seção **Rede** permite ativar ou desativar o **Firewall pessoal**.

A configuração da proteção de **Web e email** permite ativar ou desativar os seguintes componentes:

- **Controle de Web** - Bloqueia páginas da Web que possam conter material potencialmente ofensivo. Além disso, os administradores do sistema podem especificar preferências de acesso para 27 categorias de sites predefinidas.
- **Proteção do acesso à web** - Se ativada, todo o tráfego através de HTTP ou HTTPS será rastreado quanto a software malicioso.
- **Proteção do cliente de email** - Monitora a comunicação recebida através dos protocolos POP3 e IMAP.
- **Proteção antispam** - Rastreia spam ou emails não solicitados.
- **Proteção antiphishing** - Outra camada de proteção que fornece um nível superior de defesa de sites ilegítimos que tentam adquirir senhas e outras informações confidenciais.

Para desativar os módulos individuais temporariamente, clique na opção verde ao lado do módulo desejado. Observe que essa ação pode diminuir o nível de proteção do seu computador.

Para reativar a proteção do componente de segurança desativado, clique na opção vermelha para retornar um componente a seu estado ativado.

OBSERVAÇÃO: Todas as medidas protetivas desativadas dessa forma serão reativadas depois de uma reinicialização do computador.

Para acessar configurações detalhadas de um componente de segurança específico, clique no ícone de engrenagem ao lado de qualquer componente**.**

Existem opções adicionais na parte inferior da janela de configuração. Para carregar os parâmetros de configuração utilizando um arquivo de configuração *.xml* ou salvar os parâmetros atuais em um arquivo de configuração, use a opção **Importar e exportar configurações**. Para obter informações mais detalhadas, consulte Importar/Exportar configurações.

Para opções com mais detalhes, clique em **Configuração avançada** ou pressione **F5**.

3.8.1 Computador

O módulo **Computador** pode ser encontrado em **Configuração** > **Computador**. Ele exibe uma visão geral dos módulos de proteção descritos no capítulo anterior. Nesta seção, as seguintes configurações estão disponíveis:

Clique na roda de engrenagem ao lado de **Proteção em tempo real do sistema de arquivos** e clique em **Editar exclusões** para abrir a janela de configuração de exclusão, que permite a exclusão de arquivos e pastas do rastreamento.

OBSERVAÇÃO: O status de proteção do documento pode não estar disponível até que você o ative em **Configuração avançada** (F5) > **Antivírus** > **Proteção de documentos**. Depois de ativar, é preciso reiniciar seu computador no Painel de configuração > Computador clicando em **Reiniciar** sob Controle de dispositivos, ou a partir do painel Status da proteção clicando em **Reiniciar o computador**.

Pausar a Proteção antivírus e antispyware - A qualquer momento que você desativar temporariamente a Proteção antivírus e antispyware, você poderá selecionar o período de tempo para o qual deseja que o componente selecionado seja desativado usando o menu suspenso e então clicar em **Aplicar** para desativar o componente de segurança. Para reativar a proteção, clique em **Ativar proteção antivírus e antispyware**.

Configuração do rastreamento do computador... - Clique para ajustar os parâmetros do rastreamento de computador (rastreamento executado manualmente).

3.8.1.1 Antivírus

A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, emails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la, primeiro bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

Para definir configurações do módulo antivírus em detalhes, clique em **Configuração avançada** ou pressione **F5**.

As **opções do rastreamento** para todos os módulos de proteção (por exemplo, Proteção em tempo real do sistema de arquivos, Proteção do acesso à web, ...) permitem que você ative ou desative a detecção do seguinte:

- Os **aplicativos potencialmente indesejados** (PUAs) não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo.
  Leia mais sobre esses tipos de aplicativos no glossário.
- **Aplicativos potencialmente inseguros** refere-se a software comercial legítimo que tenha o potencial de ser usado indevidamente para fins maliciosos. Exemplos de aplicativos potencialmente inseguros incluem ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.
  Leia mais sobre esses tipos de aplicativos no glossário.
- **Aplicativos suspeitos** incluem programas compactados com empacotadores ou protetores. Esses tipos de protetores são frequentemente explorados por autores de malware para impedir a detecção.

A tecnologia **Anti-Stealth** é um sistema sofisticado que fornece a detecção de programas nocivos, como os rootkits, que podem se auto-ocultar do sistema operacional. Isso significa que não é possível detectá-los usando técnicas comuns de testes.

As **exclusões** permitem que você exclua arquivos e pastas do rastreamento. Recomendamos que você crie exclusões somente quando for absolutamente necessário, a fim de garantir que todos os objetos sejam rastreados contra ameaças. Há situações em que você pode precisar excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação. Para excluir um objeto do rastreamento, consulte Exclusões.

Configuração avançada - ESET Endpoint Security

Configuração avançada

ANTIVÍRUS
Proteção em tempo real do sistema de arquivos
Rastreamento sob demanda do computador
Rastreamento em estado ocioso
Rastreamento na inicialização
Mídia removível
Proteção de documentos
HIPS
ATUALIZAR
FIREWALL PESSOAL
WEB E EMAIL
CONTROLE DE DISPOSITIVO
FERRAMENTAS
INTERFACE DO USUÁRIO

BÁSICO
OPÇÕES DO SCANNER
Ativar detecção de aplicativos potencialmente não desejados
Ativar detecção de aplicativos potencialmente inseguros
Ativar detecção de aplicativos suspeitos
ANTI-STEALTH
Ativar tecnologia Anti-Stealth
EXCLUSÕES
Caminhos a serem excluídos do rastreamento
Editar
CACHE LOCAL COMPARTILHADO

Padrão
OK
Cancelar

3.8.1.1.1 Uma infiltração foi detectada

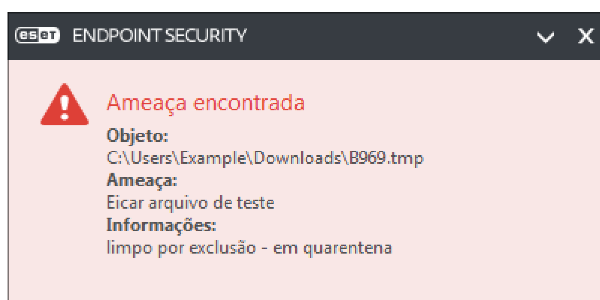
As ameaças podem alcançar o sistema a partir de vários pontos de entrada, tais como páginas da web, pastas compartilhadas, via email ou dispositivos removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.).

Comportamento padrão

Como um exemplo geral de como as infiltrações são tratadas pelo ESET Endpoint Security, as infiltrações podem ser detectadas usando:

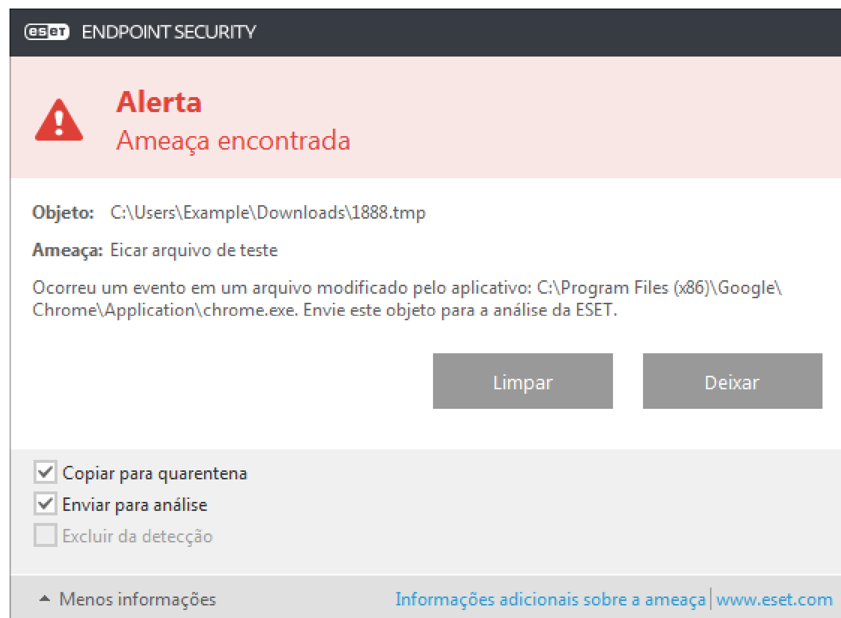
- Proteção em tempo real do sistema de arquivos
- Proteção do acesso à Web
- Proteção do cliente de email
- Rastreamento sob demanda do computador

Cada um usa o nível de limpeza padrão e tentará limpar o arquivo e movê-lo para a Quarentena ou encerrar a conexão. Uma janela de notificação é exibida na área de notificação, no canto inferior direito da tela. Para obter mais informações sobre níveis de limpeza e de comportamento, consulte Limpeza.



Limpeza e exclusão

Se não houver uma ação predefinida a ser adotada para a Proteção em tempo real do sistema de arquivos, você será solicitado a selecionar uma opção em uma janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. Não se recomenda selecionar **Nenhuma ação**, pois os arquivos infectados não serão limpos. A exceção a isso é quando você tem certeza de que um arquivo é inofensivo e foi detectado por engano.



Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo para o seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

Se um arquivo infectado estiver "bloqueado" ou em uso por um processo do sistema, ele somente será excluído após ter sido liberado (normalmente após a reinicialização do sistema).

Várias ameaças

Se quaisquer arquivos infectados não foram limpos durante um rastreamento de computador (ou o nível de limpeza estava configurado como **Sem limpeza**), será exibida uma janela de alerta solicitando a você que selecione as ações adequadas para esses arquivos. Selecione ações para os arquivos (as ações são definidas individualmente para cada arquivo na lista) e clique em **Fim**.

Exclusão de arquivos em arquivos compactados

No modo de limpeza Padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Tenha cautela ao executar um rastreamento com Limpeza rígida, com esse tipo de limpeza ativado um arquivo compactado será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência, etc., recomendamos que você faça o seguinte:

- Abra o ESET Endpoint Security e clique em Rastrear o computador.
- Clique em **Rastreamento inteligente** (para obter mais informações, consulte Rastrear o computador)
- Após a conclusão do rastreamento, revise o log para obter informações como o número de arquivos rastreados, infectados e limpos

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

3.8.1.2 Cache local compartilhado

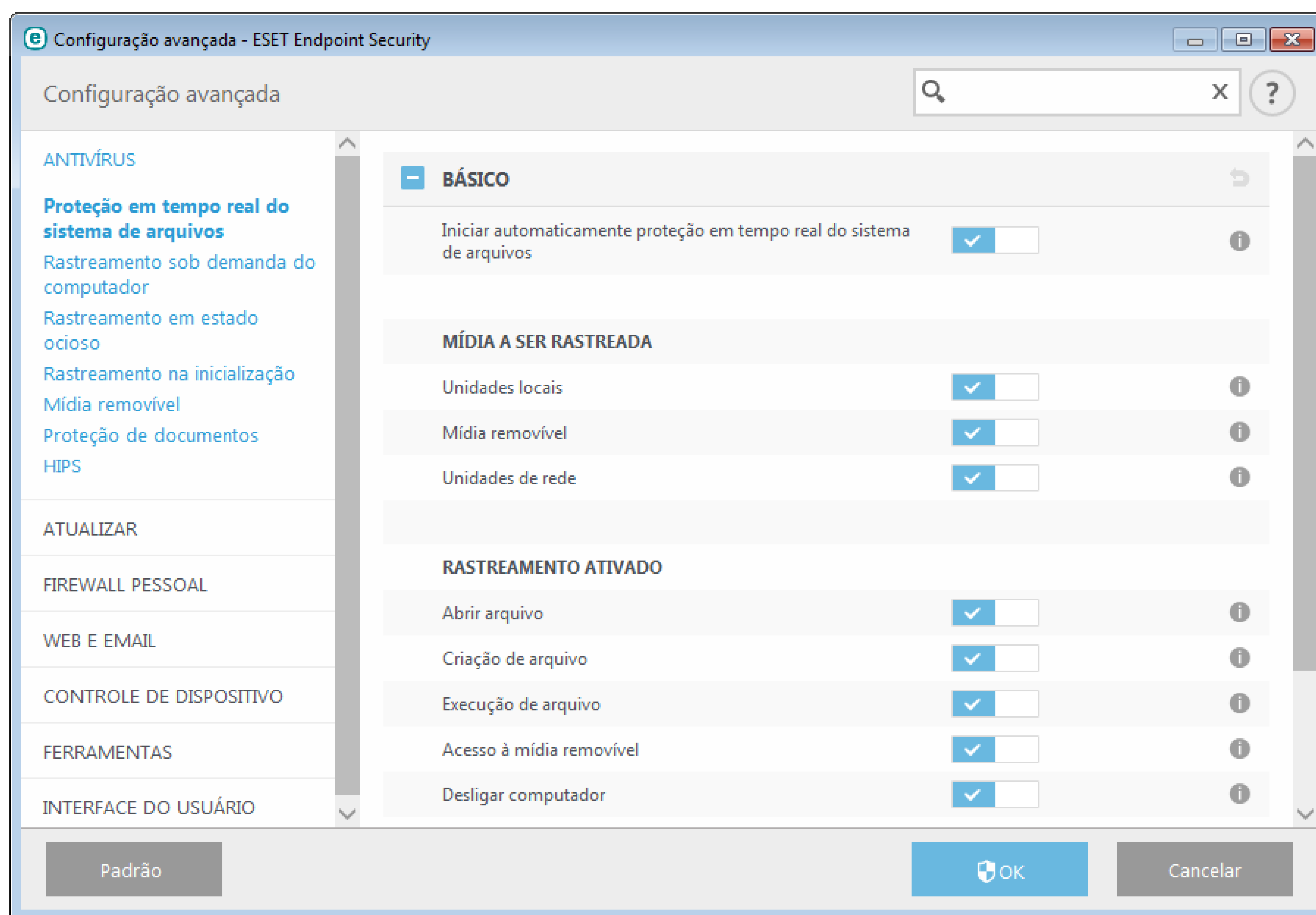
O cache local compartilhado melhorará o desempenho em ambientes virtualizados ao eliminar o rastreamento duplicado na rede. Isso garante que cada arquivo seja rastreado somente uma vez e armazenado no cache compartilhado. Ative a opção **Opção de cache** para salvar informações sobre rastreamentos de arquivos e pastas em sua rede no cache local. Se você realizar um novo rastreamento, o ESET Endpoint Security verificará se há arquivos rastreados no cache. Se os arquivos corresponderem, eles serão excluídos do rastreamento.

A configuração de **Servidor de cache** contém o seguinte:

- **Nome do host** - Nome ou endereço IP do computador no qual o cache está localizado.
- **Porta** - Número de porta usado para comunicação (mesmo que foi definido no Cache local compartilhado).
- **Senha** - Especifique a senha do Cache local compartilhado, se necessário.

3.8.1.3 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos relacionados a antivírus no sistema. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção em tempo real do sistema de arquivos é ativada na inicialização do sistema.



Por padrão, a proteção em tempo real do sistema de arquivos é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outra proteção em tempo real), a proteção em tempo real pode ser desativada desmarcando **Iniciar proteção em tempo real do sistema de arquivos automaticamente** em **Configuração avançada**, em **Proteção em tempo real do sistema de arquivos** > **Básico**.

Mídia a ser rastreada

Por padrão, todos os tipos de mídia são rastreadas quanto a potenciais ameaças:

Unidades locais - Controla todas as unidades de disco rígido do sistema.
Mídia removível - Controla CD/DVDs, armazenamento USB, dispositivos Bluetooth, etc.
Unidades de rede - Rastreia todas as unidades mapeadas.

Recomendamos que você use as configurações padrão e as modifique somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

Rastreamento ativado

Por padrão, todos os arquivos são verificados na abertura, criação ou execução. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador:

- **Abertura de arquivo** - Ativa ou desativa o rastreamento quando arquivos estiverem abertos.
- **Criação de arquivo** - Ativa ou desativa o rastreamento quando arquivos forem criados.
- **Execução de arquivo** - Ativa ou desativa o rastreamento quando arquivos forem executados.
- **Acesso à mídia removível** - Ativa ou desativa o rastreamento disparado ao acessar mídia removível em particular com espaço de armazenamento.
- **Desligar computador** - Ativa ou desativa o rastreamento acionado por desligar o computador.

A proteção em tempo real do sistema de arquivos verifica todos os tipos de mídia e é acionada por vários eventos do sistema, tais como o acesso a um arquivo. Com a utilização dos métodos de detecção da tecnologia ThreatSense (descritos na seção Configuração de parâmetros do mecanismo ThreatSense), a proteção em tempo real do sistema de arquivos pode ser configurada para tratar arquivos recém-criados de forma diferente dos arquivos existentes. Por exemplo, é possível configurar a Proteção em tempo real do sistema de arquivos para monitorar mais de perto os arquivos recém-criados.

Para garantir o impacto mínimo no sistema ao usar a proteção em tempo real, os arquivos que já foram rastreados não são rastreados repetidamente (exceto se tiverem sido modificados). Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Esse comportamento é controlado usando a **Otimização inteligente**. Se essa **Otimização inteligente** estiver desativada, todos os arquivos serão rastreados sempre que forem acessados. Para modificar essa configuração, pressione **F5** para abrir a Configuração avançada e expanda **Antivírus** > **Proteção em tempo real do sistema de arquivos**. Clique em **Parâmetro do ThreatSense**> **Outro** e marque ou desmarque **Ativar otimização inteligente**.

3.8.1.3.1 Parâmetros adicionais do ThreatSense

Parâmetros ThreatSense adicionais para arquivos criados e modificados recentemente - A probabilidade de infecção em arquivos criados ou modificados recentemente é comparativamente maior do que nos arquivos existentes. Por esse motivo, o programa verifica esses arquivos com parâmetros de rastreamento adicionais. Além dos métodos comuns de rastreamento baseados em assinaturas, também é usada a heurística avançada, que pode detectar novas ameaças antes do lançamento da atualização do banco de dados de assinatura de vírus. Além dos arquivos recém-criados, o rastreamento é executado em arquivos de autoextração (.sfx) e em empacotadores em tempo real (arquivos executáveis compactados internamente). Por padrão, os arquivos compactados são rastreados até o décimo nível de compactação e são verificados, independentemente do tamanho real deles. Para modificar as configurações de rastreamento em arquivos compactados, desative **Configurações padrão de rastreamento em arquivos compactados**.

Para saber mais sobre **Empacotadores em tempo real**, **Arquivos compactados de auto extração** e **Heurística avançada** consulte a configuração de parâmetros do mecanismo do ThreatSense.

Parâmetros ThreatSense adicionais para arquivos executados - Por padrão, a heurística avançada é usada quando os arquivos são executados. Quando ativada, é altamente recomendado manter a Otimização inteligente e o ESET Live Grid ativados para minimizar o impacto no desempenho do sistema.

3.8.1.3.2 Níveis de limpeza

A proteção em tempo real possui três níveis de limpeza (para acessar as configurações de nível de limpeza, clique em **Configuração do mecanismo ThreatSense** na seção **Proteção em tempo real do sistema de arquivos** e clique em **Limpeza**).

Sem limpeza - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

Limpeza normal - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma notificação no canto inferior direito da tela.. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá outras ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

Limpeza rígida - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, o usuário é solicitado a selecionar uma ação em uma janela de aviso.

Aviso: Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem arquivos infectados. No modo **Limpeza rígida**, o arquivo compactado seria excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

3.8.1.3.3 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.com. Este arquivo de teste é inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo está disponível para download em http://www.eicar.org/download/eicar.com

OBSERVAÇÃO: Antes de realizar um rastreamento da proteção de tempo real, é preciso desativar o firewall. Se o firewall estiver ativado, ele detectará e impedirá o download do arquivo de teste. Certifique-se de que você reative o firewall imediatamente depois de sua verificação da proteção do sistema de arquivos em tempo real.

3.8.1.3.4 Quando modificar a configuração da proteção em tempo real

A proteção do sistema de arquivos em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Seja sempre cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos.

Após a instalação do ESET Endpoint Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique em ao lado de cada guia na janela (**Configuração avançada** > **Antivírus** > **Proteção do sistema de arquivos em tempo real**).

3.8.1.3.5 O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos problemas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada

Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração** na janela principal do programa e clique em **Proteção em tempo real do sistema de arquivos**.

Se a proteção em tempo real não for ativada na inicialização do sistema, geralmente é porque **Iniciar automaticamente proteção em tempo real do sistema de arquivos** está desativada. Para ativar essa opção, navegue até **Configuração avançada** (**F5**) e clique em **Antivírus** > **Proteção em tempo real do sistema de arquivos** > **Básico**. Certifique-se de que a opção **Iniciar automaticamente proteção em tempo real do sistema de arquivos** esteja ativada.

Se a proteção em tempo real não detectar nem limpar infiltrações

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema antes da instalação da ESET.

A proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e estiver ativado **Iniciar automaticamente proteção em tempo real do sistema de arquivos**), isto pode ser devido a conflitos com outros programas. Para ajuda na resolução deste problema, entre em contato com o Atendimento ao cliente da ESET.

3.8.1.4 Rastreamento sob demanda do computador

O rastreador sob demanda é uma parte importante do ESET Endpoint Security. Ele é usado para realizar rastreamentos nos arquivos e pastas do seu computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. Recomendamos que você realize rastreamentos detalhados regulares do sistema (por exemplo, uma vez por mês) para detectar vírus que não tenham sido capturados pela Proteção em tempo real do sistema de arquivos. Isso pode acontecer se a Proteção em tempo real do sistema de arquivos estiver desativada no momento, se o banco de dados de vírus for obsoleto ou se o arquivo não for detectado como vírus ao ser salvo no disco.

Há dois tipos de **Rastrear o computador** disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

Leia Progresso do rastreamento para obter mais informações sobre o processo de rastreamento.

Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastrear o computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. A vantagem do Rastreamento inteligente é que ele é fácil de operar e não requer configuração de rastreamento detalhada. O Rastreamento inteligente verifica todos os arquivos nas unidades locais e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte Limpeza.

Rastreamento personalizado

O rastreamento personalizado é uma solução excelente, caso queira especificar parâmetros de rastreamento, como rastreamento de alvos e métodos de rastreamento. A vantagem do rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de rastreamento, selecione **Rastreamento do computador** > **Rastreamento personalizado** e selecione uma opção no menu suspenso **Alvos de rastreamento** ou selecione alvos específicos na estrutura em árvore. Um alvo de rastreamento pode ser também especificado por meio da inserção do caminho da pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione **Rastrear sem limpar**. Ao realizar um rastreamento você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Parâmetros Threatsense** > **Limpeza**.

A realização de rastreamentos de computador com o Rastreamento personalizado é adequada para usuários avançados com experiência anterior na utilização de programas antivírus.

Rastreamento de mídia removível

Semelhante ao rastreamento inteligente - inicie rapidamente um rastreamento de mídia removível (como CD/DVD/USB) atualmente conectada ao computador. Isso pode ser útil quando você conectar uma unidade flash USB a um computador e quiser rastrear seu conteúdo quanto a malware e ameaças em potencial.

Esse tipo de rastreamento também pode ser iniciado clicando em **Rastreamento personalizado** e selecionando **Mídia removível** no menu suspenso **Alvos de rastreamento** e clicando em **Rastrear**.

Você pode usar o menu suspenso **Ação após o rastreamento** para escolher a ação (Nenhuma ação, Desligar, Reiniciar e Suspender) para realizar após o rastreamento.

Ativar o desligamento após o rastreamento - Ativa um desligamento agendado quando o computador conclui o rastreamento sob demanda. Uma janela de diálogo de confirmação do desligamento aparece e permanece aberta por 60 segundos. Clique em **Cancelar** para desativar o desligamento solicitado.

OBSERVAÇÃO: Recomendamos que execute um rastrear o computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.

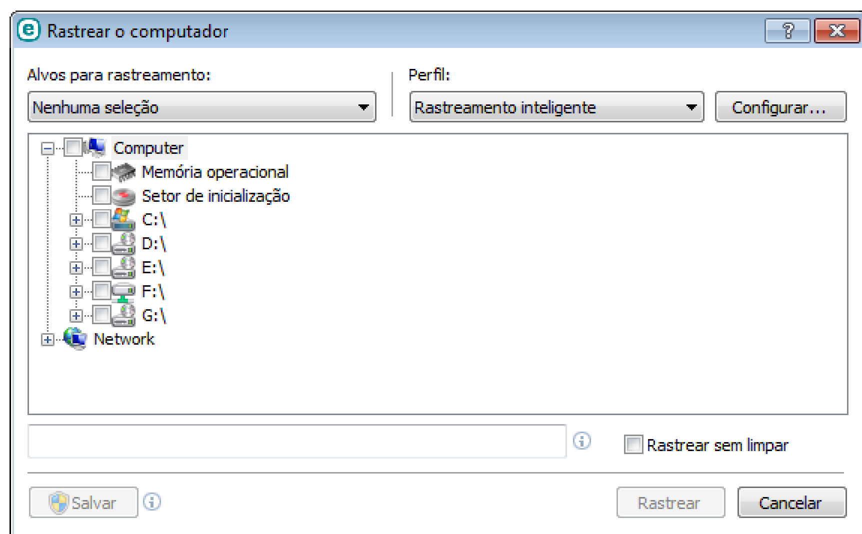
3.8.1.4.1 Iniciador de rastreamento personalizado

Se desejar verificar um alvo específico, você poderá usar a ferramenta Rastreamento personalizado clicando em **Rastrear o computador** > **Rastreamento personalizado** e selecionar uma opção no menu suspenso **Alvos de rastreamento** ou selecionar alvos específicos na estrutura de pasta (em árvore).

A janela de alvos de rastreamento permite definir que objetos (memória, unidades, setores, arquivos e pastas) são rastreados quanto a infiltrações. Selecione alvos na estrutura em árvore, que lista todos os dispositivos disponíveis no computador. O menu suspenso **Alvos de rastreamento** permite selecionar alvos de rastreamento predefinidos.

- **Por configurações de perfil** - Seleciona alvos definidos no perfil de rastreamento selecionado.
- **Mídia removível** - Seleciona disquetes, dispositivos de armazenamento USB, CD/DVD.
- **Unidades locais** - Controla todas as unidades de disco rígido do sistema.
- **Unidades de rede** - Seleciona todas as unidades de rede mapeadas.
- **Nenhuma seleção** - Cancela todas as seleções.

Para navegar rapidamente até um alvo de rastreamento selecionado ou para adicionar diretamente um alvo desejado (pasta ou arquivo(s)), digite-o no campo em branco embaixo da lista de pastas. Isso só é possível se nenhum alvo tiver sido selecionado na estrutura em árvore e se o menu **Alvos de rastreamento** estiver definido como **Nenhuma seleção**.



Os itens infectados não são limpos automaticamente. O rastreamento sem limpar pode ser usado para obter uma visão geral do status de proteção atual. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração...** > **Parâmetros Threatsense** > **Limpeza**. As informações sobre o rastreamento serão salvas em um relatório de rastreamento.

Você pode escolher um perfil no menu suspenso **Perfil de rastreamento** para ser usado para rastreamento dos alvos escolhidos. O perfil padrão é **Rastreamento inteligente**. Há mais dois perfis de rastreamento predefinidos intitulados **Rastreamento detalhado** e **Rastreamento do menu de contexto**. Estes perfis de rastreamento usam parâmetros diferentes do motor ThreatSense. Clique em **Configuração...** para configurar em detalhes o perfil de rastreamento escolhido no menu Perfil de rastreamento. As opções disponíveis são descritas na seção **Outro** na

Configuração de parâmetros do mecanismo ThreatSense.

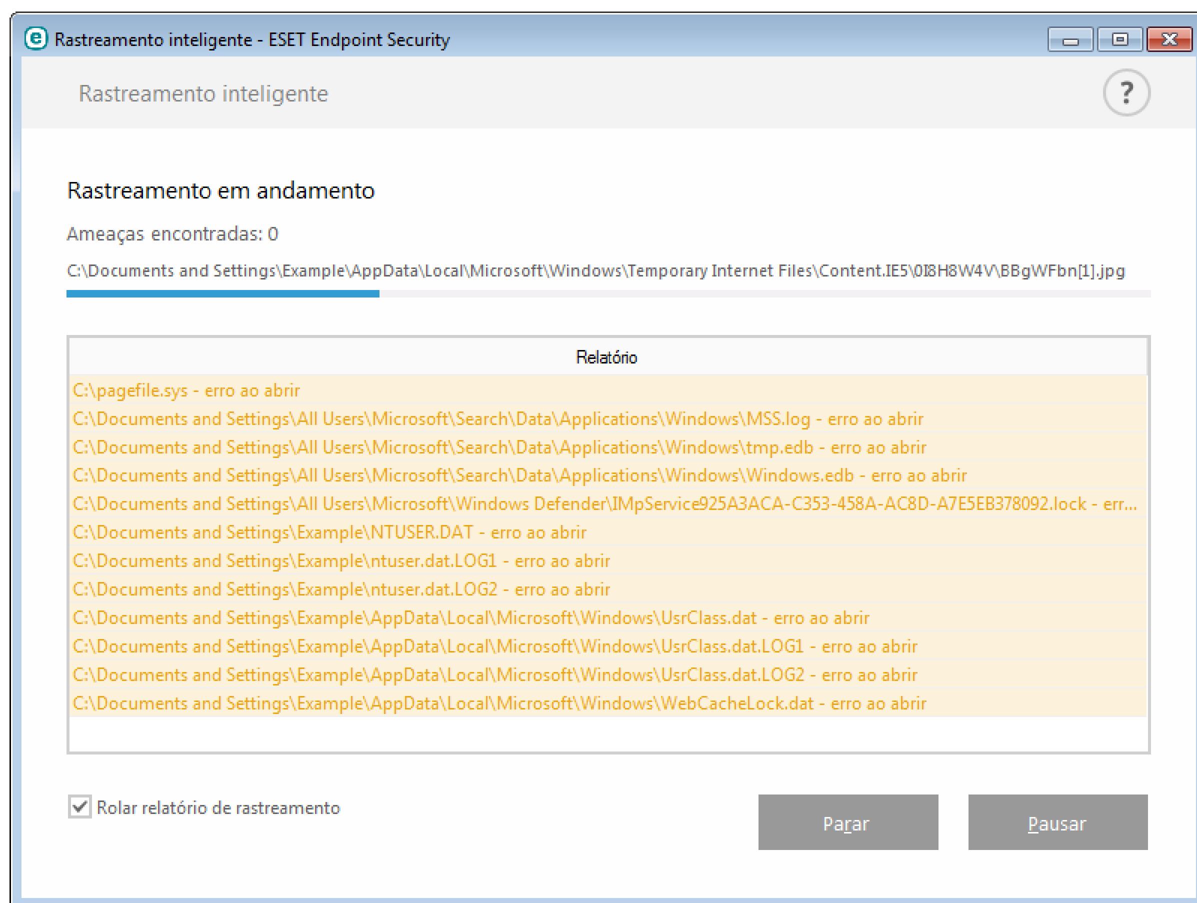
Clique em **Salvar** para salvar as alterações feitas na sua seleção de alvos, incluindo seleções feitas dentro da estrutura em árvore da pasta.

Clique em **Rastrear** para executar o rastreamento com os parâmetros personalizados definidos.

Rastrear como administrador permite que você execute o rastreamento usando a conta do administrador. Clique nessa opção se o usuário atual não tiver privilégios para acessar os arquivos apropriados para serem rastreados. Observe que esse botão não estará disponível se o usuário atual não puder acionar operações de UAC como Administrador.

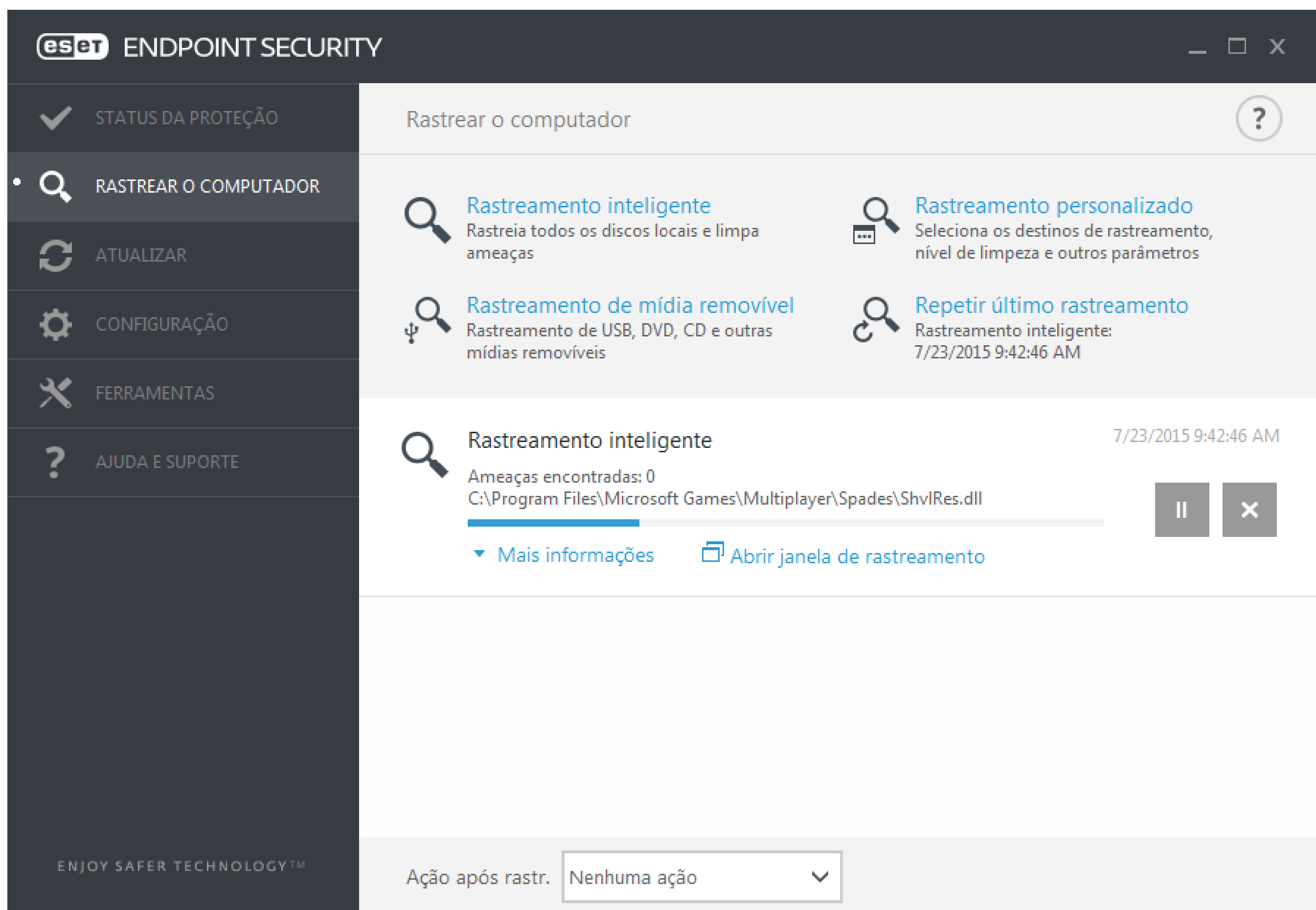
3.8.1.4.2 Progresso do rastreamento

A janela de progresso do rastreamento mostra o status atual do rastreamento e informações sobre a quantidade de arquivos encontrados que contêm código malicioso.



OBSERVAÇÃO: É normal que alguns arquivos, como arquivos protegidos por senha ou arquivos exclusivamente utilizados pelo sistema (geralmente *pagefile.sys* e determinados arquivos de log), não possam ser rastreados.

Progresso do rastreamento - A barra de progresso mostra o status de objetos já rastreados em relação aos objetos ainda aguardando para serem rastreados. O status de progresso do rastreamento é derivado do número total de objetos incluídos no rastreamento.
Destino - O nome do objeto rastreado no momento e sua localização.
Ameaças encontradas - Mostra o número total de ameaças encontradas durante um rastreamento.
Pausa - Pausa um rastreamento.
Continuar - Essa opção torna-se visível quando o progresso do rastreamento é pausado. Clique em **Continuar** para dar continuidade ao rastreamento.
Parar - Termina o rastreamento.
Percorrer log de rastreamento - Se estiver ativado, o log de rastreamento rolará automaticamente para baixo à medida que novas entradas forem adicionadas para que as entradas mais recentes fiquem visíveis.



3.8.1.5 Controle de dispositivos

O ESET Endpoint Security fornece controle automático de dispositivos (CD/DVD/USB/...). Esse módulo permite rastrear, bloquear ou ajustar filtros/permissões estendidos e define a capacidade de um usuário de acessar e trabalhar com um determinado dispositivo. Isso pode ser útil se a intenção do administrador do computador for evitar o uso de dispositivos com conteúdo não solicitado pelos usuários.

Dispositivos externos compatíveis:

- Armazenamento em disco (HDD, disco removível USB)
- CD/DVD
- Impressora USB
- Armazenamento de FireWire
- Dispositivo Bluetooth
- Leitor de cartão inteligente
- Dispositivo de imagens
- Modem
- Porta LPT/COM
- Dispositivos portáteis
- Todos os tipos de dispositivo

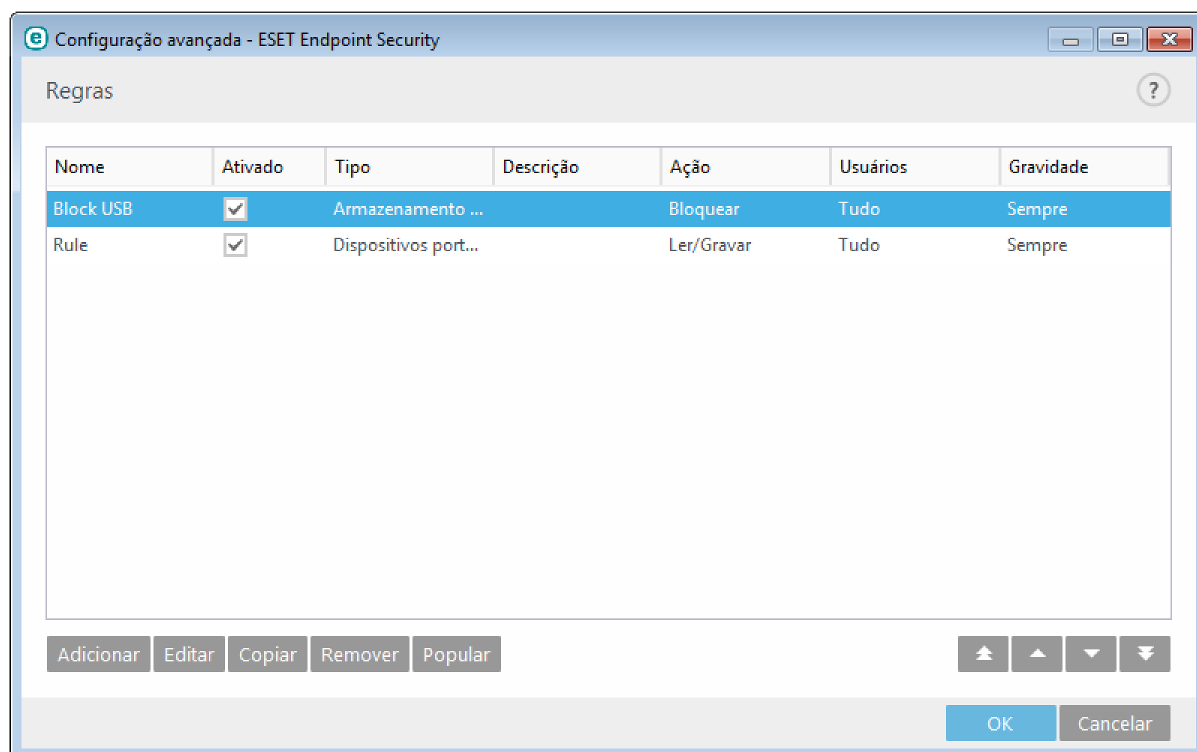
As opções de configuração do controle de dispositivos podem ser modificadas em **Configuração avançada** (F5) > **Controle de dispositivos**.

Marcar a opção ao lado de **Integrar no sistema** ativa o recurso de Controle de dispositivos no ESET Endpoint Security, você precisará reiniciar o computador para que as alterações tenham efeito. Quando o Controle de dispositivos estiver ativado, as **Regras** ficarão ativas, permitindo abrir a janela do Editor de regras.

Se um dispositivo bloqueado por uma regra existente for inserido, uma janela de notificação será exibida e o acesso ao dispositivo não será concedido.

3.8.1.5.1 Editor de regras do controle de dispositivos

A janela **Editor de regras do controle de dispositivos** mostra as regras existentes e permite que se controle de forma precisa os dispositivos externos que os usuários conectam ao computador.



Determinados dispositivos podem ser permitidos ou bloqueados de acordo com seu usuário, grupo de usuários ou com base em vários parâmetros adicionais que podem ser especificados na configuração da regra. A lista de regras contém diversas descrições de uma regra, tais como nome, tipo de dispositivo externo, ação a ser realizada após conectar um dispositivo externo ao seu computador e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique na caixa de seleção **Ativado** ao lado de uma regra para desativá-la até que você queira usá-la no futuro. Selecione uma ou mais regras e clique em **Remover** para excluir a(s) regra(s) permanentemente.

Copiar - Cria uma nova regra com opções predefinidas usadas para outra regra selecionada.

Clique em **Preencher** para preencher automaticamente os parâmetros do dispositivo de mídia removível para dispositivos conectados ao computador.

As regras são listadas por ordem de prioridade, com regras de prioridade superior mais próximas do início. Regras podem ser movidas clicando em **Topo/Cima/Baixo/Fundo** e podem ser movidas individualmente ou em grupos.

O relatório de controle de dispositivos registra todas as ocorrências nas quais o controle de dispositivos é acionado. As entradas de logs podem ser visualizadas a partir da janela principal do programa do ESET Endpoint Security em **Ferramentas** > Relatórios.

3.8.1.5.2 Adição de regras do controle de dispositivos

Uma Regra de controle de dispositivos define a ação a ser tomada quando um dispositivo que corresponde aos critérios da regra é conectado ao computador.

Configuração avançada - ESET Endpoint Security

Editar regra

Nome: Block USB
Regra ativada
Tipo de dispositivo: Armazenamento em disco
Ação: Bloquear
Tipo de critério: Dispositivo
Fabricante
Modelo
Número de série
Gravidade do registro em log: Sempre
Lista de usuários: Editar
OK

Insira uma descrição da regra no campo **Nome** para melhor identificação. Clique na opção ao lado de **Regra ativada** para ativar ou desativar esta regra. Isso pode ser útil caso não deseje excluir a regra permanentemente.

Tipo de dispositivo

Escolha o tipo de dispositivo externo no menu suspenso (Armazenamento em disco/Dispositivo portátil/Bluetooth/FireWire/...). As informações sobre o tipo de dispositivo são coletadas do sistema operacional e podem ser visualizados no Gerenciador de dispositivos do sistema se um dispositivo estiver conectado ao computador. Os dispositivos de armazenamento incluem discos externos ou leitores de cartão de memória convencionais conectados via USB ou FireWire. Leitores de cartões inteligentes abrangem todos os leitores de cartões inteligentes com um circuito integrado incorporado, como cartões SIM ou cartões de autenticação. Scanners e câmeras são exemplos de dispositivos de imagens. Como esses dispositivos oferecem apenas informações sobre suas ações e não oferecem informações sobre os usuários, eles só podem ser bloqueados de forma global.

Ação

O acesso a dispositivos que não sejam de armazenamento pode ser permitido ou bloqueado. Por outro lado, as regras de dispositivos de armazenamento permitem a seleção de uma das seguintes configurações de direitos:

- **Ler/Gravar** - Será permitido acesso total ao dispositivo.
- **Bloquear** - O acesso ao dispositivo será bloqueado.
- **Apenas leitura** - Será permitido acesso apenas para leitura ao dispositivo.
- **Alertar** - Cada vez que um dispositivo for conectado, o usuário será notificado se ele é permitido ou bloqueado, e um registro no log será feito. Dispositivos não são lembrados, uma notificação continuará a ser exibida com conexões subsequentes ao mesmo dispositivo.

Note que nem todas as ações (permissões) estão disponíveis para todos os tipos de dispositivos. Se for um dispositivo do tipo armazenamento, todas as quatro Ações estão disponíveis. Para dispositivos sem armazenamento, haverá somente duas (por exemplo, **Somente leitura** não estará disponível para Bluetooth, o que significa que dispositivos de Bluetooth poderão apenas ser permitidos, bloqueados ou alertados).

Tipo de critério - Selecione **Grupo do dispositivo** ou **Dispositivo.**

Outros parâmetros mostrados a seguir podem ser usados para ajustar as regras e adequá-las a dispositivos. Todos os parâmetros não fazem diferenciação entre letras maiúsculas e minúsculas:

- **Fabricante** - Filtragem por nome ou ID do fabricante.
- **Modelo** - O nome específico do dispositivo.
- **Número de série** - Os dispositivos externos geralmente têm seus próprios números de série. No caso de CD/DVD, este é o número de série da mídia em si, e não o da unidade de CD.

OBSERVAÇÃO: Se esses parâmetros estiverem indefinidos, a regra irá ignorar estes campos enquanto faz a correspondência. Os parâmetros de filtragem em todos os campos de texto não fazem diferenciação de maiúsculas e minúsculas; caracteres curinga (*, ?) não são aceitos.

DICA: Para ver informações sobre um dispositivo, crie uma regra para o tipo de dispositivos, conecte o dispositivo ao seu computador e, em seguida, verifique os detalhes do dispositivo no Relatório de controle de dispositivos.

Gravidade

- **Sempre** - criar relatório de todos os eventos.
- **Diagnóstico** - Registra informações necessárias para ajustar o programa.
- **Informações** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Aviso** - Registra mensagens de erros críticos e de aviso.
- **Nenhum** - Nenhum registro será feito.

As regras podem ser limitadas a determinados usuários ou grupos de usuários adicionando-os à **Lista de usuários**:

- **Adicionar** - Abre os **Tipos de objeto: Usuários ou Grupos** que permite selecionar os usuários desejados.
- **Remover** - Remove o usuário selecionado do filtro.

OBSERVAÇÃO: Todos os dispositivos podem ser filtrados por regras do usuário (por exemplo, dispositivos de criação de imagem não fornecem informações sobre usuários, apenas sobre ações).

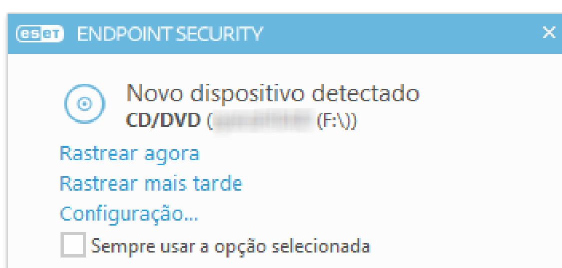
3.8.1.6 Mídia removível

O ESET Endpoint Security fornece rastreamento automático de mídia removível (CD/DVD/USB/...). Este módulo permite que você rastreie uma mídia inserida. Isso pode ser útil se a intenção do administrador do computador for evitar que os usuários usem uma mídia removível com conteúdo não solicitado.

Ação a ser executada após inserção da mídia removível - Selecione a ação padrão que será desenvolvida quando um dispositivo de mídia removível for inserido no computador (CD/DVD/USB). Se a opção **Mostrar opções de rastreamento** for selecionada, será exibida uma notificação que lhe permite selecionar a ação desejada:

- **Não rastrear** - Nenhuma ação será executada e a janela **Novo dispositivo detectado** será fechada.
- **Rastreamento automático de dispositivo** - Um rastreamento do computador sob demanda do dispositivo de mídia removível inserido será executado.
- **Mostrar opções de rastreamento** - Abre a seção de configuração da mídia removível.

Quando uma mídia removível for inserida, a caixa de diálogo a seguir será exibida:



Rastrear agora - Isto vai acionar o rastreamento da mídia removível.

Rastrear mais tarde - O rastreamento da mídia removível será adiado.

Configuração - Abre a Configuração avançada.

Sempre usar a opção selecionada - Quando estiver selecionado, a mesma ação será executada quando uma mídia removível for inserida outra vez.

Além disso, o ESET Endpoint Security tem o recurso de Controle de dispositivos, que permite que você defina regras de utilização de dispositivos externos em um determinado computador. Acesse a seção Controle de dispositivos para obter mais detalhes sobre o controle de dispositivos.

3.8.1.7 Rastreamento em estado ocioso

Você pode ativar o scanner em estado ocioso em **Configuração avançada** em **Antivírus** > **Rastreamento em estado ocioso** > **Básico**. Defina a opção ao lado de **Ativar rastreamento em estado ocioso** como **Ativado** para ativar esse recurso. Quando o computador estiver em estado ocioso, um rastreamento sem segundo plano do computador será realizado em todas as unidades locais. Veja Acionadores de detecção de estado ocioso para uma lista completa de condições que devem ser cumpridas para acionar o rastreamento de estado ocioso.

Por padrão, o rastreamento de estado ocioso não será executado quando o computador estiver fazendo uso de bateria. Você pode substituir essa configuração ativando a chave ao lado de **Executar mesmo se o computador estiver na bateria** na Configuração avançada.

Ative a opção **Ativar registro** na Configuração avançada para registrar uma saída de rastreamento do computador na seção Relatórios (a partir da janela principal do programa, clique em **Ferramentas** > **Relatórios** e selecione **Rastreamento do computador** a partir do menu suspenso **Log**).

A detecção em estado ocioso será executada quando o computador estiver em um dos seguintes estados:

- Proteção de tela
- Computador bloqueado
- Logoff de usuário

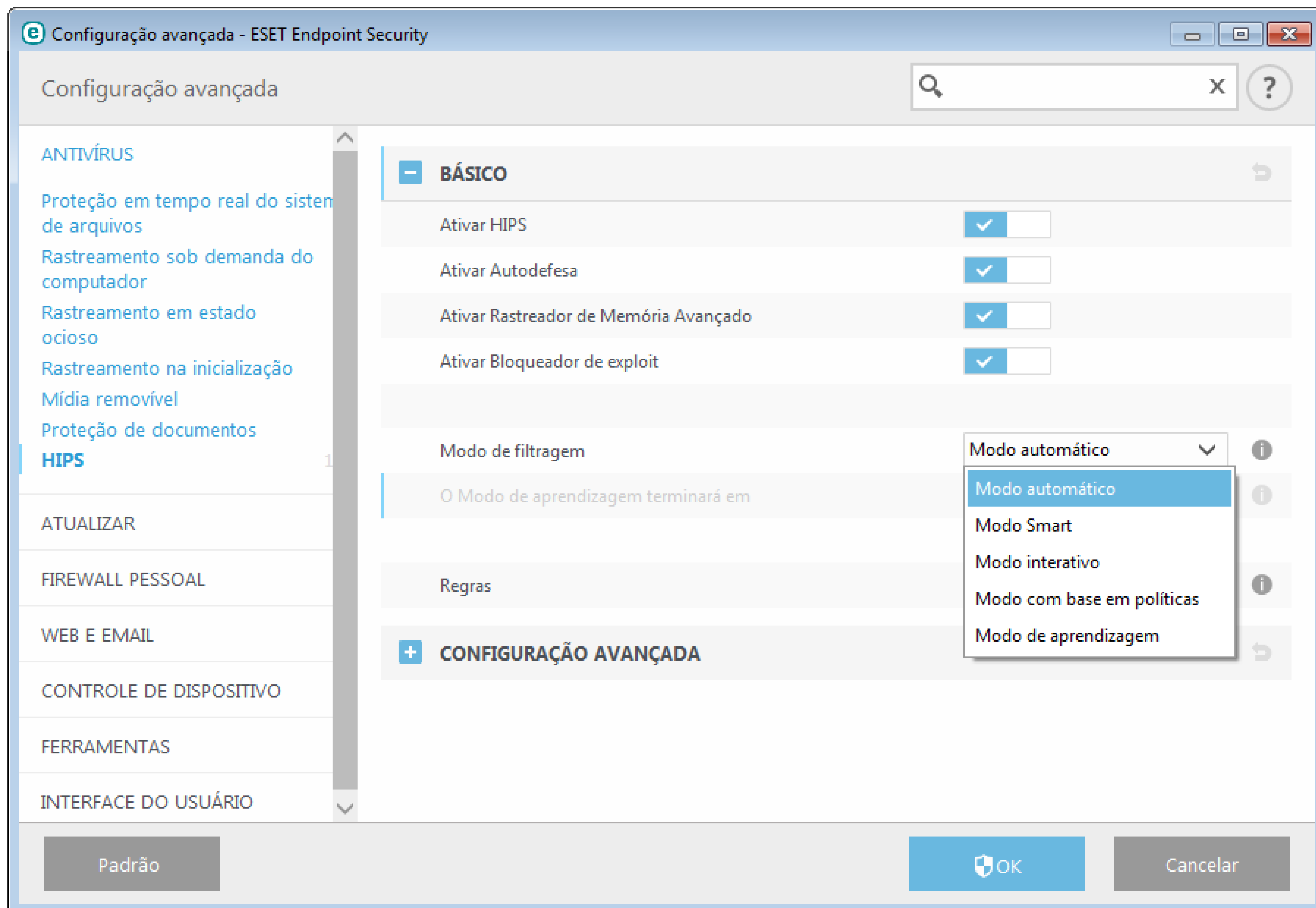
Clique na Configuração de parâmetros do mecanismo ThreatSense para modificar parâmetros de verificação (p. ex., métodos de detecção) para o scanner no estado ocioso.

3.8.1.8 Sistema de prevenção de intrusos de host (HIPS)


Apenas um usuário experiente deve fazer alterações nas configurações do HIPS. A configuração incorreta das configurações HIPS pode causar instabilidade no sistema.

O **Sistema de prevenção de intrusos de host** (HIPS) protege o sistema de malware ou de qualquer atividade que tentar prejudicar a segurança do computador. Ele utiliza a análise comportamental avançada em conjunto com as capacidades de detecção de filtro de rede para monitorar processos em execução, arquivos e chaves de registro. O HIPS é separado da proteção em tempo real do sistema de arquivos e não é um firewall; ele monitora somente processos em execução no sistema operacional.

As configurações HIPS podem ser encontradas em **Configuração avançada** (F5) > **Antivírus** > **HIPS** > **Básico**. O status do HIPS (ativado/desativado) é exibido na janela do programa principal do ESET Endpoint Security, em **Configuração** > **Computador**.



o ESET Endpoint Security usa uma tecnologia de Autodefesa incorporada para impedir que o software malicioso danifique ou desabilite a proteção antivírus e antispyware. Dessa forma, você poderá ter certeza que seu sistema está protegido o tempo todo. É preciso reiniciar o Windows para desativar o HIPS ou a Autodefesa.

O **Rastreamento de memória avançado** funciona combinado com o Bloqueio de exploit para fortalecer a proteção contra malware feito para evitar a detecção por produtos antimalware através do uso de ofuscação ou criptografia. Por padrão, o scanner de memória avançado está ativado. Leia mais sobre esse tipo de proteção no glossário.

O **Bloqueio de exploit** é feito para fortalecer tipos de aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email e componentes do MS Office. Por padrão, o bloqueio de exploit está ativado. Leia mais sobre esse tipo de proteção no glossário.

A filtragem pode ser executada em um de quatro modos:

Modo automático - As operações são ativadas, exceto aquelas bloqueadas por regras predefinidas que protegem o sistema.

Modo interativo - O sistema solicitará que o usuário confirme as operações.

Modo com base em políticas - As operações são bloqueadas.

Modo de aprendizagem - As operações são ativadas e uma regra é criada após cada operação. As regras criadas nesse modo podem ser visualizadas no Editor de regras, mas sua prioridade é menor que a prioridade das regras criadas manualmente ou das regras criadas no modo automático. Quando selecionar o Modo de aprendizagem do menu suspenso Modo de filtragem HIPS, a configuração **Modo de aprendizagem vai terminar em** ficará disponível. Selecione a duração pela qual você deseja se envolver no módulo de aprendizado, a duração máxima é de 14 dias. Quando a duração especificada tiver terminado, você será solicitado a editar as regras criadas pelo HIPS enquanto ele estava no modo de aprendizagem. Você também pode escolher um modo de filtragem diferente, ou adiar a decisão e continuar usando o modo de aprendizagem.

Modo Inteligente - O usuário será notificado apenas sobre eventos muito suspeitos.

O sistema HIPS monitora os eventos dentro do sistema operacional e reage a eles de acordo com regras similares às regras usadas no firewall pessoal. Clique em **Editar** para abrir a janela de gerenciamento de regras do HIPS. Aqui é

possível selecionar, criar, editar ou excluir regras.

No exemplo a seguir demonstraremos como restringir o comportamento indesejado de aplicativos:

1. Nomeie a regra e selecione **Bloquear** no menu suspenso **Ação**.
2. Ative a opção **Notificar usuário** para exibir uma notificação sempre que uma regra for aplicada.
3. Selecione pelo menos uma operação para a qual a regra será aplicada. Na janela **Aplicativos de origem**, selecione **Todos os aplicativos** no menu suspenso para aplicar sua nova regra a todos os aplicativos que tentarem realizar qualquer das operações de aplicativo nos aplicativos especificados.
4. Selecione **Alterar estado de outro aplicativo**(todas as operações são descritas na ajuda do produto, que pode ser acessada pressionando F1).
5. Selecione **Aplicativos específicos** no menu suspenso e **Adicione** um ou vários aplicativos que deseja proteger.
6. Clique em **Concluir** para salvar sua nova regra.

3.8.1.8.1 Configuração avançada

As opções a seguir são úteis para depurar e analisar o comportamento de um aplicativo:

Drivers sempre com permissão para carregar - Os drivers selecionados sempre tem permissão para carregar, independente do modo de filtragem configurado, a menos que explicitamente bloqueado pela regra do usuário.

Registrar todas as operações bloqueadas - Todas as operações bloqueadas serão gravadas no log HIPS.

Notificar quando ocorrerem alterações nos aplicativos de Inicialização - Exibe uma notificação na área de trabalho toda vez que um aplicativo for adicionado ou removido da inicialização do sistema.

Consulte nosso artigo da Base de conhecimento para obter uma versão atualizada desta página de ajuda.

3.8.1.8.2 Janela interativa HIPS

Se a ação padrão para uma regra estiver definida como **Perguntar**, uma janela de diálogo será exibida sempre que a regra for acionada. Você pode optar por **Negar** ou **Permitir** a operação. Se você não definir uma ação no tempo determinado, uma nova ação será selecionada com base nas regras.

A janela da caixa de diálogo permite que você crie uma regra com base em qualquer nova ação que o HIPS detectar e então definirá as condições nas quais permitir ou negar essa ação. Os parâmetros exatos podem ser definidos depois de clicar em **Mostrar opções**. As regras criadas como esta são consideradas iguais às regras criadas manualmente, portanto a regra criada a partir de uma janela de diálogo pode ser menos específica que a regra que acionou a janela de diálogo. Isso significa que após a criação dessa regra, a mesma operação pode acionar a mesma janela.

Lembrar temporariamente desta ação para este processo faz com que a ação (**Permitir/Negar**) seja utilizada até que ocorra uma alteração de regras ou o modo de filtragem ou ocorra uma atualização do módulo do HIPS ou reinicialização do sistema. Depois de qualquer uma dessas três ações, as regras temporárias serão excluídas.

3.8.1.9 Modo de apresentação

O modo de apresentação é um recurso para usuários que pretendem usar o seu software continuamente sem serem perturbados por janelas pop-up e que ainda pretendem reduzir o uso da CPU. Ele também pode ser utilizado durante apresentações que não podem ser interrompidas pela atividade do antivírus. Quando ativado, todas as janelas pop-up são desativadas e tarefas agendadas não são executadas. A proteção do sistema ainda é executada em segundo plano, mas não requer interação com nenhum usuário.

Clique em **Configuração** > **Computador** e então clique na opção ao lado de **Modo de apresentação** para ativar o modo de apresentação manualmente. Na **Configuração avançada** (F5), clique em **Ferramentas** > **Modo de apresentação** e clique na opção ao lado de **Ativar automaticamente o modo de apresentação ao executar aplicativos em tela cheia** para que o ESET Endpoint Security ative o modo de apresentação automaticamente quando aplicativos em tela cheia forem executados. Ativar automaticamente o modo de apresentação é um risco de segurança em potencial, pois o ícone do status de proteção na barra de tarefas ficará laranja e exibirá um aviso. Esse aviso também pode ser visto na janela do programa principal, onde a opção **Modo de apresentação ativado** será exibida em laranja.

Quando a opção **Ativar automaticamente o modo de apresentação ao executar aplicativos em tela cheia** for

marcada, o modo de apresentação será iniciado depois que você iniciar um aplicativo em tela cheia e será interrompido automaticamente ao sair do aplicativo. Esse recurso é especialmente útil para iniciar o modo de apresentação logo após iniciar um jogo, abrir um aplicativo em tela cheia ou iniciar uma apresentação.

Você também pode selecionar **Desativar o modo de apresentação automaticamente após** para definir o período de tempo em minutos após o qual o modo de apresentação será desativado automaticamente.

OBSERVAÇÃO: se o firewall pessoal estiver no modo interativo e o modo de apresentação for ativado, você pode ter dificuldades para conectar-se à Internet. Isso pode ser um problema se você iniciar um jogo on-line. Normalmente, você será solicitado a confirmar tal ação (se não houver regras de comunicação ou exceções definidas), mas a interação com o usuário fará com que o modo de apresentação seja desativado. A solução é definir uma regra de comunicação para cada aplicativo que possa estar em conflito com esse comportamento ou usar outro Modo de filtragem no firewall pessoal. Tenha em mente que, se o modo de apresentação estiver ativado e você acessar uma página da web ou um aplicativo que possa ser considerado um risco à segurança, eles poderão ser bloqueados e nenhuma explicação ou aviso serão exibidos devido à desativação da interação com o usuário.

3.8.1.10 Rastreamento na inicialização

Por padrão o rastreamento automático de arquivo na inicialização será executado na inicialização do sistema e durante a atualização do banco de dados de assinatura de vírus. Esse rastreamento depende das Tarefas e configurações da agenda.

As opções de rastreamento na inicialização são parte de uma tarefa da agenda da **Rastreamento de arquivo na inicialização do sistema**. Para modificar suas configurações de rastreamento na inicialização, vá até **Ferramentas** > **Agenda**, clique em **Verificação automática de arquivos de inicialização** e então em **Editar...**. Na última etapa, a janela Rastreamento automático de arquivo na inicialização será exibida (consulte o capítulo a seguir para obter mais detalhes).

Para obter mais instruções sobre o gerenciamento e a criação de tarefas da Agenda, consulte Criação de novas tarefas.

3.8.1.10.1 Rastreamento de arquivos em execução durante inicialização do sistema

Ao criar uma tarefa agendada de Rastreamento de arquivo na inicialização do sistema, você tem várias opções para ajustar os seguintes parâmetros:

O menu suspenso **Arquivos usados comumente** especifica a profundidade do rastreamento da execução de arquivos na inicialização do sistema. Os arquivos são organizados em ordem decrescente de acordo com os seguintes critérios:

- **Todos os arquivos registrados** (mais arquivos rastreados)
- **Arquivos usados raramente**
- **Arquivos usados comumente**
- **Arquivos usados com frequência**
- **Somente os arquivos mais frequentemente usados** (últimos arquivos rastreados)

Dois grupos específicos também estão inclusos:

- **Arquivos executados antes do logon do usuário** - Contém arquivos de locais que podem ser acessados sem que o usuário esteja conectado (inclui quase todos os locais de inicialização, tais como serviços, objetos auxiliares do navegador, notificação de Winlogon, entradas da Agenda do Windows, dlls conhecidos, etc.).
- **Arquivos executados após o logon do usuário** - Contém arquivos de locais que podem ser acessados após um usuário se conectar (inclui arquivos que são executados somente para um usuário específico, normalmente arquivos em *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

As listas de arquivos a serem rastreados estão fixas para cada grupo anteriormente.

Prioridade do rastreamento - O nível de prioridade usado para determinar quando um rastreamento iniciará:

- **Quando em espera** - a tarefa será realizada somente quando o sistema estiver em espera,
- **Mais baixa** - quando a carga do sistema é a menor possível,
- **Baixa** - em uma carga baixa do sistema,
- **Normal** - em uma carga média do sistema.

3.8.1.11 Proteção de documentos

O recurso de proteção de documentos verifica os documentos do Microsoft Office antes de eles serem abertos, bem como arquivos obtidos por download automaticamente pelo Internet Explorer, tais como elementos do Microsoft ActiveX. A proteção de documentos fornece uma camada de proteção além da proteção do sistema de arquivos em tempo real, bem como pode ser desativada para aprimorar o desempenho em sistemas não expostos a um alto volume de documentos do Microsoft Office.

Integrar ao sistema ativa o sistema de proteção. Para modificar essa opção, pressione F5 para abrir a janela Configuração avançada e clique em **Antivírus** > **Proteção de documentos** na árvore Configuração avançada.

Este recurso é ativado por aplicativos que utilizam o Microsoft Antivirus API (por exemplo, Microsoft Office 2000 e superior ou Microsoft Internet Explorer 5.0 e superior).

3.8.1.12 Exclusões

As exclusões permitem que você exclua arquivos e pastas do rastreamento. Recomendamos que você crie exclusões somente quando for absolutamente necessário, a fim de garantir que todos os objetos sejam rastreados contra ameaças. Há situações em que você pode precisar excluir um objeto. Por exemplo, entradas extensas do banco de dados que diminuem o desempenho do computador durante o rastreamento ou um software que entra em conflito com a verificação (por exemplo, software de backup).

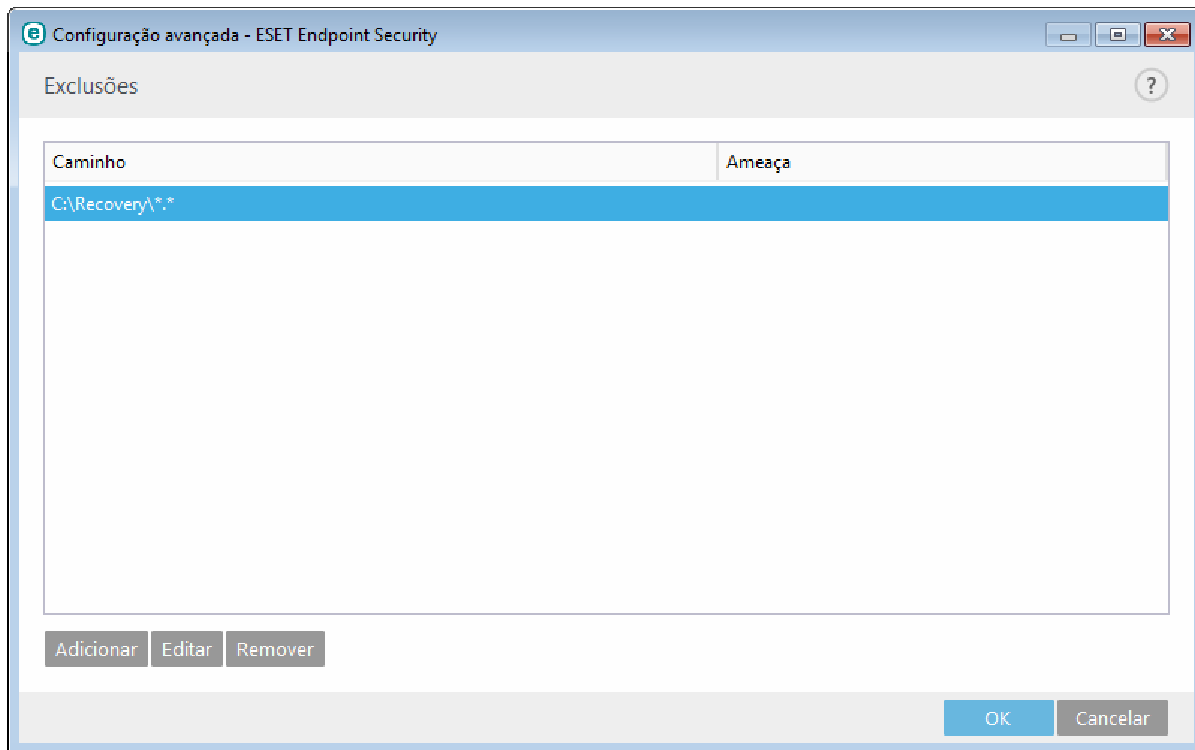
Para excluir um objeto do rastreamento:

1. Clique em **Adicionar**,
2. Digite o caminho para um objeto ou selecione-o na estrutura em árvore.

Você pode usar caracteres curinga para abranger um grupo de arquivos. Um ponto de interrogação (?) representa um caractere de variável único e um asterisco (*) representa uma cadeia de caracteres variável, com zero ou mais caracteres.

Exemplos

- Se você desejar excluir todos os arquivos em uma pasta, digite o caminho para a pasta e use a máscara “*.*”.
- Para excluir a unidade por completo, incluindo todos os arquivos e subpastas, use a máscara "D:*".
- Se você desejar excluir somente arquivos doc, use a máscara “*.doc”.
- Se o nome de um arquivo executável tiver um determinado número de caracteres (e os caracteres variarem) e você souber somente o primeiro com certeza (digamos, “D”), use o seguinte formato: "D????.exe". Os sinais de interrogação substituem os caracteres em falta (desconhecidos).



OBSERVAÇÃO: uma ameaça em um arquivo não será detectada pelo módulo de proteção em tempo real do sistema de arquivos ou módulo de rastreamento do computador se um arquivo atender aos critérios para exclusão do rastreamento.

Colunas

Caminho - caminho para arquivos e pastas excluídos.

Ameaça - se houver um nome de uma ameaça exibido ao lado de um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça. Se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus. Esse tipo de exclusão pode ser utilizado apenas para determinados tipos de infiltrações e pode ser criado na janela de alerta de ameaças que informa a infiltração (clique em **Mostrar opções avançadas** e selecione **Excluir da detecção**) ou clicando em **Ferramentas** > **Quarentena**, clicando com o botão direito do mouse no arquivo em quarentena e selecionando **Restaurar e excluir da detecção** no menu de contexto.

Elementos de controle

Adicionar - exclui objetos da detecção.

Editar - permite que você edite as entradas selecionadas.

Remover - remove as entradas selecionadas.

3.8.1.13 Configuração de parâmetros do mecanismo ThreatSense

o ThreatSense é a tecnologia que consiste em muitos métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante a propagação inicial de uma nova ameaça. Ela utiliza uma combinação de análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina os rootkits com êxito.

as opções de configuração do motor ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados.
- A combinação de diversos métodos de detecção.
- Níveis de limpeza etc.

Para acessar a janela de configuração, clique em **Configuração de parâmetro do mecanismo ThreatSense** na janela de Configuração avançada de qualquer módulo que use a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos,
- Rastreamento em estado ocioso,
- Rastreamento na inicialização,
- Proteção de documentos,
- Proteção do cliente de email,
- Proteção do acesso à web,
- Rastrear o computador.

Os parâmetros do ThreatSense são altamente otimizados para cada módulo, e modificá-los pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre verificar empacotadores em tempo real ou ativar a heurística avançada no módulo de Proteção em tempo real do sistema de arquivos pode resultar em maior utilização dos recursos (normalmente, somente arquivos recém-criados são verificados utilizando esses métodos). Recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto Rastrear o computador.

Objetos a serem rastreados

Esta seção permite definir quais componentes e arquivos do computador serão rastreados quanto a infiltrações.

Memória operacional - Rastreia procurando ameaças que atacam a memória operacional do sistema.

Setores de inicialização - Rastreia os setores de inicialização quanto à presença de vírus no registro de inicialização principal.

Arquivos de email - O programa oferece suporte às seguintes extensões: DBX (Outlook Express) e EML.

Arquivos compactados - O programa oferece suporte às seguintes extensões: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e muitas outras.

Arquivos compactados de autoextração - Os arquivos compactados de autoextração (SFX, Self-extracting archives) são arquivos compactados que não requerem programas especializados - arquivos compactados - para se descompactarem.

Empacotadores em tempo real - Depois da execução, os empacotadores em tempo real (ao contrário dos arquivos compactados padrão) fazem a descompactação na memória. Além dos empacotadores estáticos padrão (UPX, yoda, ASPack, FSG etc.), o scanner é compatível com o reconhecimento de vários tipos adicionais de empacotadores graças à emulação do código.

Opções de rastreamento

Selecione os métodos a serem utilizados durante o rastreamento do sistema para verificar infiltrações. As opções disponíveis são:

Heurística - Uma heurística é um algoritmo que analisa a atividade (maliciosa) dos programas. A principal vantagem dessa tecnologia é a capacidade de identificar software malicioso que não existia ou que não era conhecido pelo banco de dados das assinaturas de vírus anterior. A desvantagem é uma probabilidade (muito pequena) de alarmes falsos.

Heurística avançada/DNA/Assinaturas inteligentes - A heurística avançada consiste em um algoritmo de heurística exclusivo desenvolvido pela ESET, otimizado para detecção de worms e cavalos de troia no computador e escrito em linguagens de programação de alto nível. O uso de heurística avançada aumenta muito as capacidades de detecção de ameaças de produtos ESET. As assinaturas podem detectar e identificar vírus com segurança. Usando o sistema de atualização automática, novas assinaturas são disponibilizadas em poucas horas depois da descoberta da ameaça. A desvantagem das assinaturas é que elas detectam somente os vírus que conhecem (ou suas versões levemente modificadas).

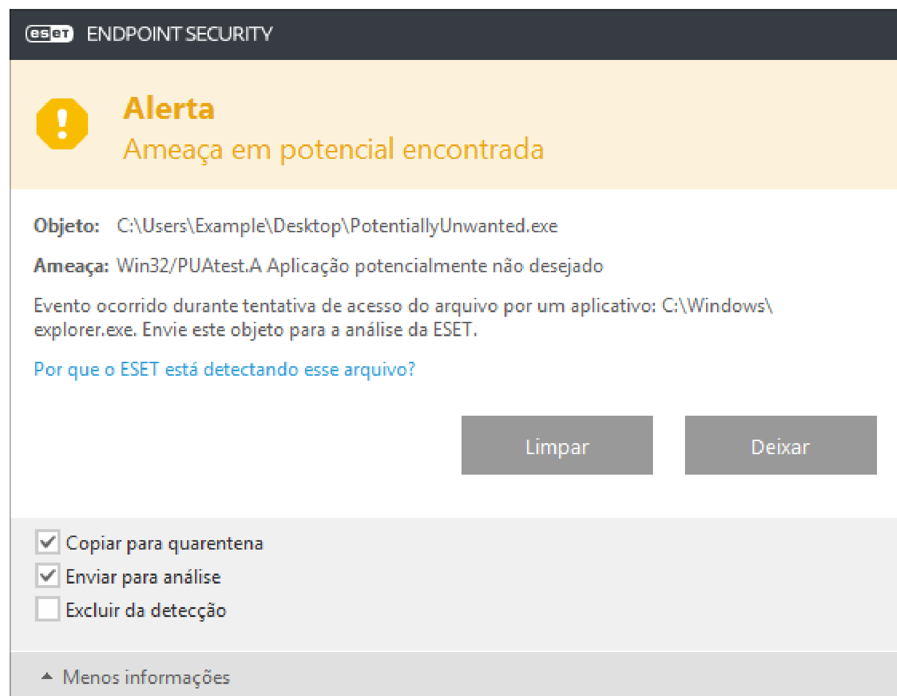
Um aplicativo potencialmente indesejado é um programa que contém adware, instala barras de ferramentas ou tem

outros objetivos pouco claros. Existem algumas situações em um usuário pode sentir que os benefícios do aplicativo potencialmente indesejado superam os riscos. Por isso, a ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso, como cavalos de Troia ou worms.

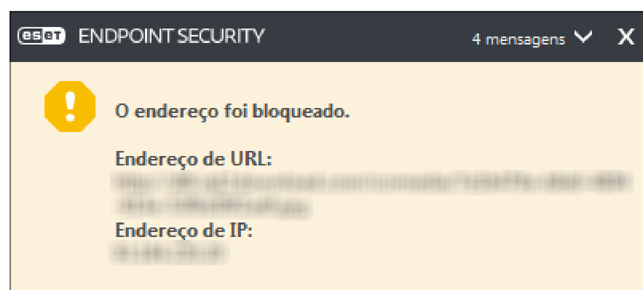
Aviso - Ameaça em potencial encontrada

Quando um aplicativo potencialmente indesejado é detectado, você poderá decidir qual ação realizar:

1. **Limpar/Desconectar**: Esta opção encerra a ação e evita que uma possível ameaça entre no sistema.
2. **Deixar**: Essa opção permite que a ameaça em potencial entre em seu sistema.
3. Para permitir que o aplicativo seja executado no seu computador no futuro sem interrupções, clique em **Mais informações/Exibir opções avançadas** e selecione a caixa de seleção ao lado de **Excluir da detecção**.

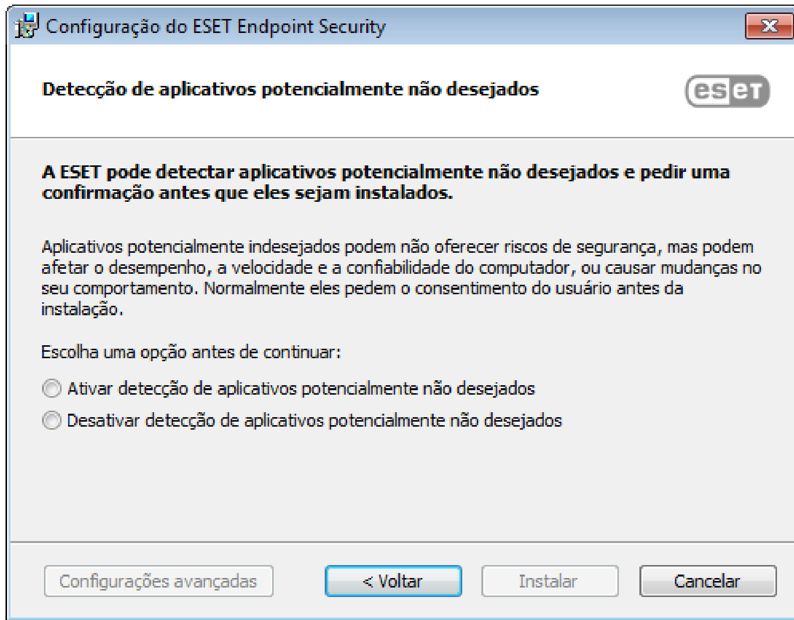


Quando um aplicativo potencialmente indesejado é detectado e não é possível limpar, uma janela de notificação **O endereço foi bloqueado** será exibida no canto inferior direito da tela. Para mais informações sobre este evento vá para **Ferramentas** > **Relatórios** > **Sites filtrados** no menu principal.



Aplicativos potencialmente indesejados - Configurações

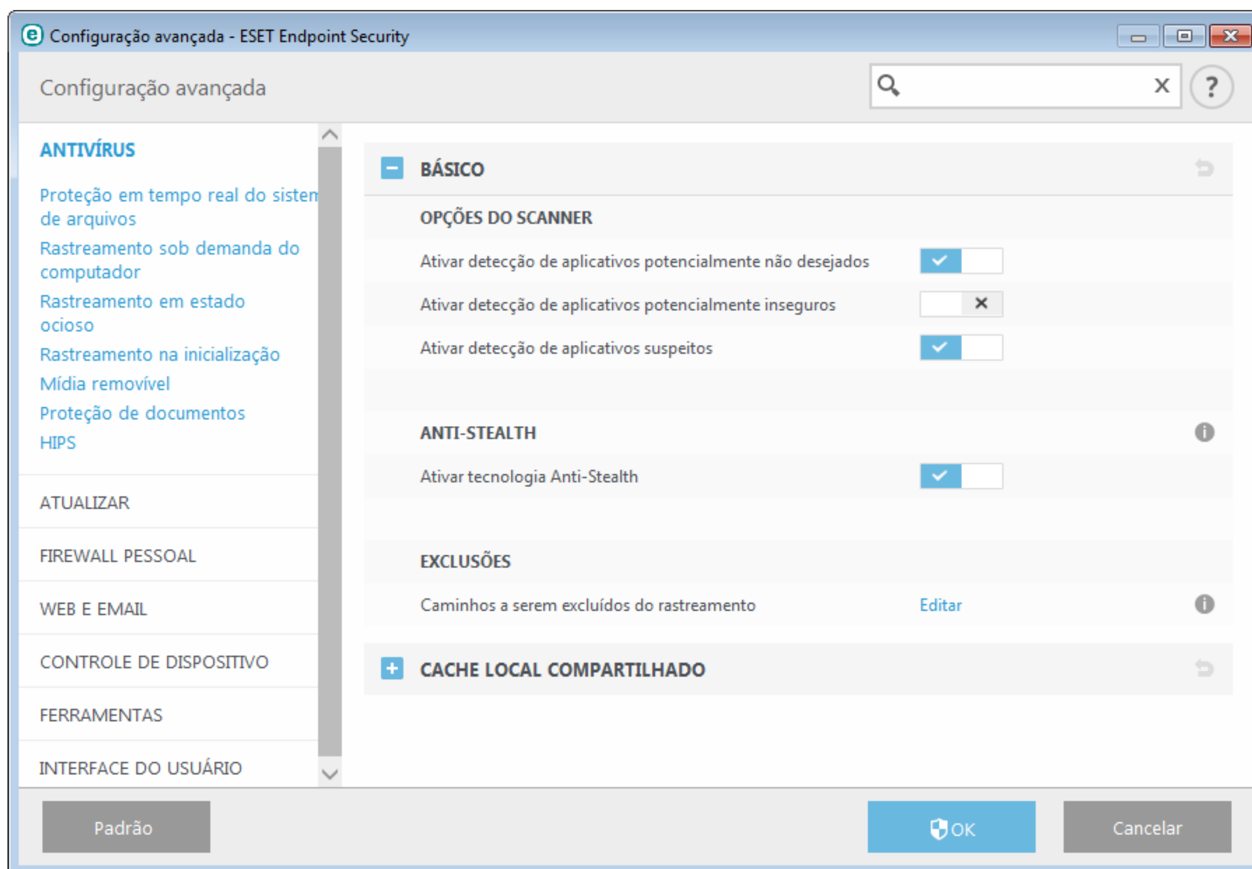
Ao instalar seu produto ESET, é possível decidir se vai ativar a detecção de aplicativos potencialmente não desejados, conforme exibido abaixo:



 Aplicativos potencialmente indesejados podem instalar adware, barras de ferramentas ou ter outros recursos de programa indesejados e inseguros.

Essas configurações podem ser modificadas nas suas configurações de programa a qualquer momento. Para ativar ou desativar a detecção de Aplicativos potencialmente indesejados, inseguros ou suspeitos, siga essas instruções:

1. Abra seu produto ESET. Como abrir meu produto ESET?
2. Pressione a tecla **F5** para acessar a **Configuração avançada**.
3. Clique em **Antivírus** e ative ou desative as opções **Ativar detecção de aplicativos potencialmente não desejados**, **Ativar detecção de aplicativos potencialmente inseguros** e **Ativar detecção de Ativar detecção de aplicativos suspeitos** de acordo com suas preferências. Confirme clicando em **OK**.



Aplicativos potencialmente indesejados - Wrapper de software

Um wrapper de software é um tipo especial de modificação de aplicativo que é usado por alguns sites de hospedagem de arquivos. É uma ferramenta de terceiros que instala o programa que você planejou baixar, mas adiciona outros software, como barras de ferramentas ou adware. O software adicional também pode fazer alterações na página inicial do seu navegador ou nas configurações de pesquisa. Além disso, sites de hospedagem de arquivos muitas vezes não notificam o fabricante do software ou receptor do download que modificações foram feitas e não permite que seja possível optar por não obter uma modificação com facilidade. Por esses motivos, a ESET classifica wrapper de software como um tipo de aplicativo potencialmente indesejado para permitir aos usuários aceitarem ou não seu download.

Consulte o seguinte artigo da Base de Conhecimento ESET para obter uma versão atualizada desta página de ajuda.

Aplicativos potencialmente inseguros - Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Ela inclui programas como ferramentas de acesso remoto, aplicativos que descobrem senhas e registradores de teclado (programas que gravam cada pressão de tecla feita por um usuário). Essa opção está desativada por padrão.

Limpeza

As configurações de limpeza determinam o comportamento do scanner enquanto limpa os arquivos infectados. Há três níveis de limpeza:

Sem limpeza - Os arquivos infectados não serão limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação. Esse nível foi desenvolvido para os usuários mais avançados que sabem o que fazer no caso de uma infiltração.

Limpeza normal - O programa tentará limpar ou excluir automaticamente um arquivo infectado com base em uma ação predefinida (dependendo do tipo de infiltração). A detecção e a exclusão de um arquivo infectado são assinaladas por uma notificação no canto inferior direito da tela.. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá outras ações de acompanhamento. O mesmo ocorre quando uma ação predefinida não pode ser concluída.

Limpeza rígida - O programa limpará ou excluirá todos os arquivos infectados. As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, o usuário é solicitado a selecionar uma ação em uma janela de aviso.

Aviso: Se um arquivo compactado tiver um ou mais arquivos infectados, haverá duas opções para tratar o arquivo. No modo padrão (Limpeza padrão), o arquivo completo será excluído se todos os arquivos que ele contém forem arquivos infectados. No modo **Limpeza rígida**, o arquivo compactado seria excluído se tiver, pelo menos, um arquivo infectado, qualquer que seja o status dos outros arquivos no arquivo compactado.

Exclusões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Outros

Ao configurar os parâmetros do mecanismo ThreatSense para um rastreamento sob demanda do computador, as seguintes opções na seção **Outro** também estarão disponíveis:

Rastrear fluxos dados alternativos (ADS) - Fluxos de dados alternativos usados pelo sistema de arquivos NTFS são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

Executar rastreamento em segundo plano com baixa prioridade - Cada sequência de rastreamento consome determinada quantidade de recursos do sistema. Se você estiver trabalhando com programas que exigem pesados recursos do sistema, você poderá ativar o rastreamento de baixa prioridade em segundo plano e economizar recursos para os aplicativos.

Registrar todos os objetos - Se essa opção estiver selecionada, o arquivo de log mostrará todos os arquivos rastreados, mesmo os que não estiverem infectados. Por exemplo, se uma infiltração for encontrada dentro de um arquivo compactado, o log também listará os arquivos limpos contidos dentro do arquivo compactado.

Ativar otimização inteligente - Com a Otimização inteligente ativada, as configurações mais ideais são utilizadas para garantir o nível mais eficiente de rastreamento, mantendo simultaneamente a velocidade de rastreamento mais alta. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento e os aplicando a tipos específicos de arquivos. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.

Manter último registro de acesso - Selecione essa opção para manter o tempo de acesso original dos arquivos rastreados, em vez de atualizá-lo (por exemplo, para uso com sistemas de backup de dados).

Limites

A seção Limites permite especificar o tamanho máximo de objetos e nível de compactação de arquivos compactados a serem rastreados:

Configurações do objeto

Tamanho máximo do objeto - Define o tamanho máximo de objetos a serem rastreados. O módulo antivírus determinado rastreará apenas objetos menores que o tamanho especificado. Essa opção apenas será alterada por usuários avançados que podem ter razões específicas para excluir objetos maiores do rastreamento. Valor padrão: *sem limite*.

Tempo máximo do rastreamento para objeto (s) - Define o valor de tempo máximo para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento. Valor padrão: *sem limite*.

Configuração de rastreamento em arquivos compactados

Nível de compactação de arquivos compactados - Especifica a profundidade máxima do rastreamento de arquivos compactados. Valor padrão: *10*.

Tamanho máximo do arquivo no arquivo compactado - Essa opção permite especificar o tamanho máximo de arquivos para os arquivos contidos em arquivos compactados (quando são extraídos) a serem rastreados. Valor

padrão: *sem limite*.

OBSERVAÇÃO: Não recomendamos alterar os valores padrão; sob circunstâncias normais, não haverá razão para modificá-los.

3.8.1.13.1 Exclusões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Essa seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento.

A exclusão de arquivos será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa que está usando certas extensões. Por exemplo, pode ser aconselhável excluir as extensões .edb, .eml e .tmp ao usar os servidores Microsoft Exchange.

Com os botões **Adicionar** e **Remover**, você pode autorizar ou proibir o rastreamento de extensões de arquivos específicas. Para adicionar uma nova extensão à lista, clique em **Adicionar**, digite a extensão no campo em branco e clique em **OK**. Quando você selecionar **Inserir valores múltiplos**, você poderá adicionar várias extensões de arquivos delimitadas por linhas, vírgulas ou ponto e vírgulas. Quando a seleção múltipla estiver ativada, extensões serão mostradas na lista. Selecione uma extensão na lista e clique em **Remover** para excluir essa extensão da lista. Se você quiser editar uma extensão selecionada, clique em **Editar**.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco representa qualquer string de caracteres e o ponto de interrogação representa qualquer símbolo.

3.8.2 Rede

O firewall pessoal controla todo o tráfego de rede para e a partir do sistema. Isso é realizado através da permissão ou proibição de conexões individuais de rede, com base em suas regras de filtragem. Ele fornece proteção contra ataques de computadores remotos e ativa o bloqueio de alguns serviços possivelmente perigosos. O Firewall pessoal também fornece funcionalidade IDS/IPS inspecionando o conteúdo de tráfego de rede permitido e bloqueando o tráfego que é considerado potencialmente nocivo.

A configuração do **firewall pessoal** pode se encontrada no painel **Configurar** em **Rede**. Aqui você pode ajustar o modo de filtragem do Firewall pessoal da ESET. Você também pode acessar mais configurações detalhadas clicando na roda de engrenagem > **Configurar** ao lado de **Firewall pessoal** ou pressionando **F5** para acessar Configuração avançada.

Proteção contra ataque de rede (IDS) - Analisa o conteúdo do tráfego da rede e protege contra ataques de rede. Qualquer tráfego que seja considerado perigoso será bloqueado. Você pode desativar a Proteção contra ataque de rede por um período de tempo específico ao clicar em .

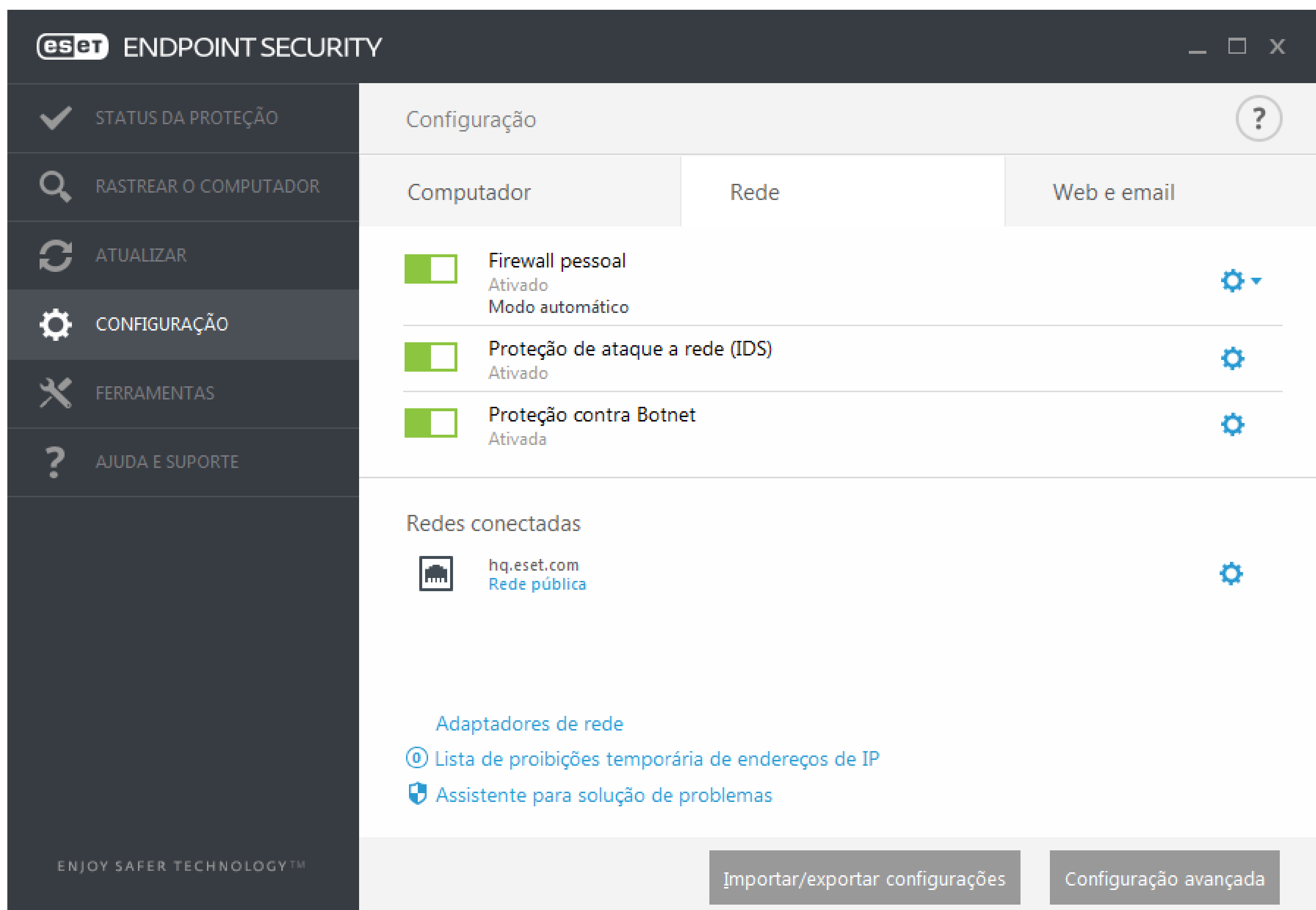
Proteção contra botnet - identifica malware de forma rápida e precisa no sistema. Você pode desativar a Proteção contra botnet por um período de tempo específico ao clicar em .

Redes conectadas - Mostra as redes às quais os adaptadores de rede estão conectados. Depois de clicar na roda de engrenagem, será solicitado que você selecione um tipo de proteção para a rede à qual você está conectado via seu adaptador de rede.

Adaptadores de rede - Aqui você pode ver cada adaptador de rede e seu perfil de firewall e zona confiável atribuídos. Para obter informações mais detalhadas, consulte Adaptadores de rede.

Lista de proibições temporária de endereços de IP - Veja uma lista de endereços de IP que foram detectados como a fonte de ataques e adicionados à lista de proibições para bloquear a conexão por um período de tempo. Para mais informações, clique nessa opção e pressione F1.

Assistente de solução de problemas - Ajuda a resolver problemas de conectividade causados pelo Firewall pessoal da ESET. Para obter informações mais detalhadas, consulte Assistente de solução de problemas.



Clique na roda de engrenagem ⚙ ao lado do **Firewall pessoal** para acessar as seguintes configurações:

Configurar... - Abre a janela Firewall pessoal na Configuração avançada, que permite definir como o firewall tratará a comunicação de rede.

Bloquear todo o tráfego - Todas as comunicação de entrada e saída serão bloqueadas pelo firewall pessoal. Utilize essa opção somente se suspeitar de riscos de segurança críticos que requeiram a desconexão do sistema da rede. Embora a filtragem de tráfego de rede esteja no modo **Bloquear todo o tráfego**, clique em **Parar de bloquear todo o tráfego** para restaurar o firewall para operação normal.

Pausar firewall (permitir todo o tráfego) - O contrário do bloqueio de todo o tráfego de rede. Se ela for selecionada, todas as opções de filtragem do firewall pessoal serão desativadas, e todas as conexões de entrada e de saída serão permitidas. Embora a filtragem de tráfego de rede esteja neste modo, clique em **Ativar firewall** para para reativar o firewall.

Modo automático - (quando outro modo de filtragem está ativado) - Clique para trocar o modo de filtragem para modo de filtragem automático (com regras definidas pelo usuário).

Modo interativo - (quando outro modo de filtragem está ativado) - Clique para trocar o modo de filtragem para modo de filtragem interativo.

3.8.2.1 Firewall pessoal

O firewall pessoal controla todo o tráfego de rede para e a partir do sistema. Isso é realizado através da permissão ou proibição de conexões individuais de rede, com base em regras de filtragem especificadas. Ele fornece proteção contra ataques de computadores remotos e ativa o bloqueio de alguns serviços. Ele também fornece proteção antivírus para protocolos HTTP, POP3 e IMAP. Esta funcionalidade representa um elemento muito importante na segurança do computador.

Ativar Proteção contra ataque de rede (IDS) - Analisa o conteúdo do tráfego da rede e protege contra ataques de rede. Qualquer tráfego que seja considerado perigoso será bloqueado.

Ativar proteção Botnet - Detecta e bloqueia comunicação com comandos maliciosos e servidores de controle com

base em padrões típicos quando o computador está infectado e um bot está tentando se comunicar.

Quatro modos de filtragem estão disponíveis para o firewall pessoal do ESET Endpoint Security. As configurações de modos de filtragem podem ser encontradas em **Configuração avançada** (F5) clicando em **Firewall pessoal**. O comportamento do firewall é alterado com base no modo de filtragem. Os modos de filtragem também influenciam o nível de interação necessário do usuário.

A filtragem pode ser executada em um de quatro modos:

Modo automático - O modo padrão. Esse modo é adequado para usuários que preferem o uso fácil e conveniente do firewall sem nenhuma necessidade de definir regras. Regras personalizadas e definidas pelo usuário podem ser criadas, mas não são exigidas no modo automático. O modo automático permite todo tráfego de saída para o sistema e bloqueia a maioria do tráfego de entrada (exceto algum tráfego da zona confiável, como permitido em IDS e opções avançadas/serviços permitidos e tráfego de entrada respondendo a comunicação de saída recente para o mesmo site remoto).

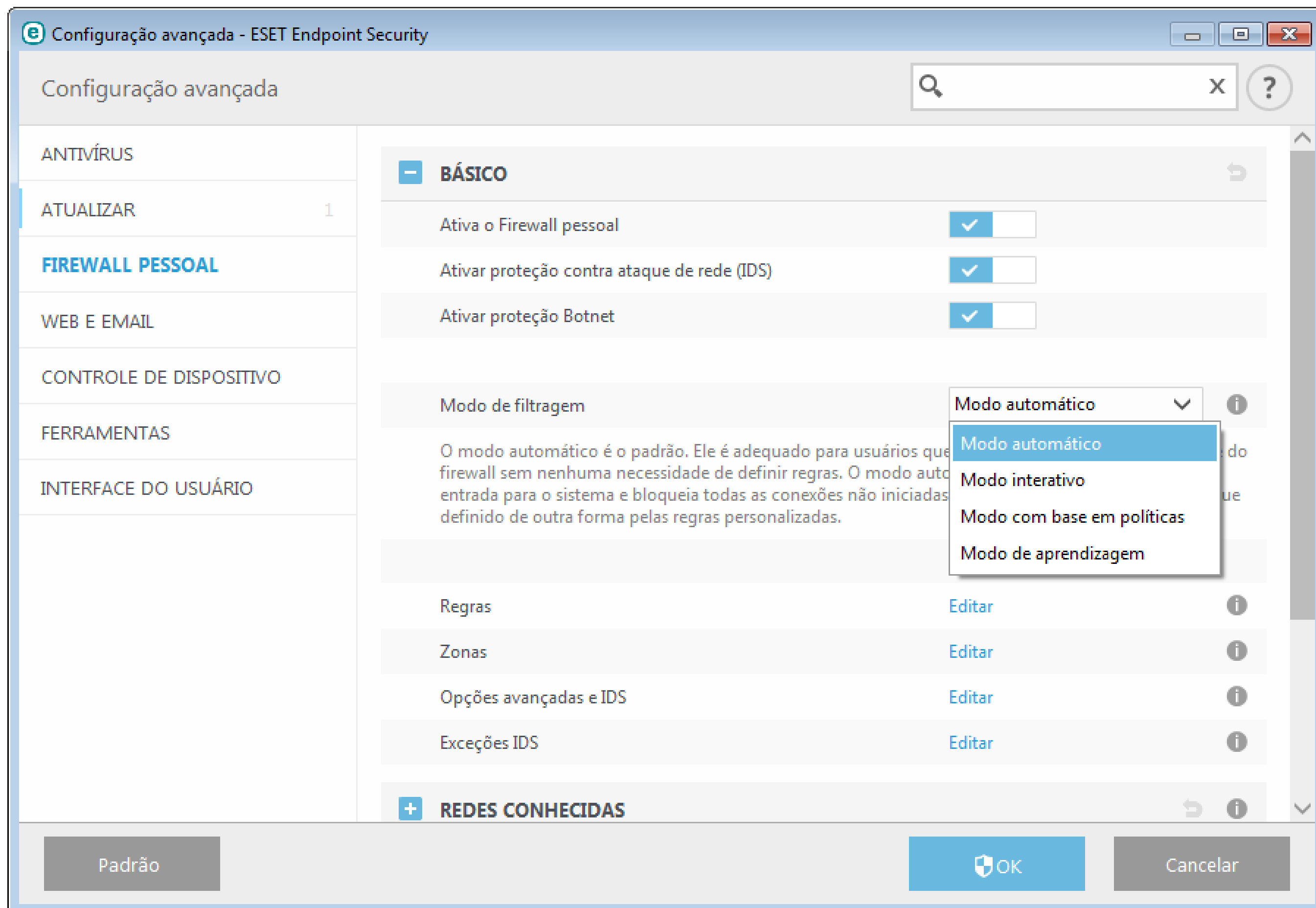
Modo interativo - Permite que você crie uma configuração personalizada para seu firewall pessoal. Quando uma comunicação para a qual não há regras aplicadas for detectada, será exibida uma janela de diálogo com a informação de uma conexão desconhecida. A janela de diálogo dá a opção de permitir ou negar a comunicação, e a decisão de permitir ou negar pode ser salva como uma nova regra para o firewall pessoal. Se o usuário escolher criar uma nova regra, todas as futuras conexões desse tipo serão permitidas ou bloqueadas de acordo com essa regra.

Modo com base em políticas - Bloqueia todas as conexões que não são definidas por uma regra específica que as permite. Esse modo permite que os usuários avançados definam as regras que permitem apenas as conexões desejadas e seguras. Todas as outras conexões não especificadas serão bloqueadas pelo firewall pessoal.

Modo de aprendizagem - Cria e salva automaticamente as regras e é adequado para a configuração inicial do firewall pessoal. Nenhuma interação com o usuário é exigida, porque o ESET Endpoint Security salva as regras de acordo com os parâmetros predefinidos. O modo de aprendizagem não é seguro e deve ser apenas usado até que todas as regras para as comunicações exigidas tenham sido criadas.

Perfis podem ser usados para personalizar o comportamento do firewall pessoal da ESET Endpoint Security ao especificar diferentes conjuntos de regras em diferentes situações.

Avaliar também regras de firewall do Windows - No modo automático, permite que o tráfego de entrada seja autorizado pelo Firewall do Windows a menos que seja bloqueado pelas regras de firewall pessoal.



Regras - Aqui você pode adicionar regras e definir como o Firewall pessoal processará o tráfego de rede.

Zonas - Aqui você pode criar zonas que consistem em vários endereços IP.

IDS e opções avançadas - Permite configurar opções avançadas de filtro e a funcionalidade IDS (usada para detectar vários tipos de ataques e vulnerabilidades).

Exceções IDS - Permite adicionar exceções IDS e personalizar reações a atividades maliciosas.

3.8.2.1.1 Modo de aprendizagem

O modo de aprendizagem cria e salva automaticamente uma regra para cada comunicação que foi estabelecida no sistema. Nenhuma interação com o usuário é exigida, porque o ESET Endpoint Security salva as regras de acordo com os parâmetros predefinidos.

Esse modo pode expor seu sistema a risco e é recomendado somente para configuração inicial do firewall pessoal.

Ative o Modo de aprendizagem em **Configuração avançada** (F5) > **Firewall pessoal** > **Configurações do modo de aprendizagem** para exibir as opções do Modo de aprendizagem. Essa seção inclui os seguintes itens:

Aviso: Enquanto está no Modo de aprendizagem, o firewall pessoal não filtra a comunicação. Todas as comunicações de saída e de entrada são permitidas. Nesse modo, o seu computador não está totalmente protegido pelo firewall pessoal.

Tipo de comunicação - Selecione os parâmetros específicos de criação de regras para cada tipo de comunicação. Há quatro tipos de comunicação:

- **Tráfego de entrada da zona Confiável** - Um exemplo de uma conexão de entrada na zona confiável seria um computador remoto a partir do qual a zona confiável está tentando estabelecer comunicação com um aplicativo local em execução no seu computador.

- **Tráfego de saída para zona Confiável** - Um aplicativo local está tentando estabelecer uma conexão com outro computador na rede local ou em uma rede na zona confiável.

- **Tráfego de entrada da Internet** - Um computador remoto tentando se comunicar com um aplicativo em execução no computador.

- **Tráfego de saída da Internet** - Um aplicativo local está tentando estabelecer uma conexão com outro computador.

Cada seção permite que você defina parâmetros a serem adicionados às regras recém-criadas:

Adicionar porta local - Inclui o número da porta local da comunicação de rede. Para as comunicações de saída, números aleatórios são frequentemente gerados. Por essa razão, recomendamos a ativação dessa opção apenas para as comunicações de entrada.

Adicionar aplicativo - Inclui o nome do aplicativo local. Essa opção é adequada para regras de nível de aplicativo (regras que definem a comunicação para um aplicativo inteiro). Por exemplo, é possível ativar a comunicação apenas para um navegador da Web ou cliente de email.

Adicionar porta remota - Inclui o número da porta remota da comunicação de rede. Por exemplo, você pode permitir ou negar um serviço específico associado a um número de porta padrão (HTTP - 80, POP3 - 110, etc.).

Adicionar endereço IP remoto/Zona confiável - Um endereço IP ou uma zona remoto(a) pode ser utilizado(a) como um parâmetro para novas regras que definem todas as conexões de rede entre o sistema local e esse endereço/ zona remoto(a). Essa opção é adequada se você desejar definir ações para determinado computador ou grupo de computadores conectados em rede.

Número máximo de regras diferentes para um aplicativo - Se um aplicativo comunicar por meio de diferentes portas para vários endereços IP etc., o firewall no modo de aprendizagem criará uma contagem apropriada de regras para esse aplicativo. Essa opção permite limitar o número de regras que podem ser criadas para um aplicativo.

3.8.2.2 Perfis do firewall

Os perfis podem ser usados para controlar o comportamento do firewall pessoal do ESET Endpoint Security. Ao criar ou editar uma regra de firewall pessoal, você pode atribuí-la a um perfil específico ou aplicá-la a cada perfil. Quando um perfil está ativo em uma interface de rede, apenas as regras globais (regras sem nenhum perfil especificado) e as regras que foram atribuídas a esse perfil são aplicadas a ele. Você pode criar vários perfis com regras diferentes atribuídas a adaptadores de rede ou atribuídas a redes para alterar com facilidade o comportamento do firewall pessoal.

Clique em **Editar** ao lado de **Lista de perfis** para abrir a janela **Perfis do firewall**, onde é possível editar perfis.

Um adaptador de rede pode ser configurado para usar um perfil configurado para uma rede específica quando estiver conectado a essa rede. Você também pode atribuir um perfil específico para uso quando em uma determinada rede em **Configuração avançada** (F5) > **Firewall pessoal** > **Redes conhecidas**. Selecione uma rede da lista de **Redes conhecidas** e clique em **Editar** para atribuir um perfil de firewall para a rede específica no menu suspenso **Perfil de firewall**. Se essa rede não tiver um perfil atribuído, então o perfil padrão do adaptador será usado. Se o adaptador for configurado para usar o perfil da rede, seu perfil padrão será usado, independentemente de à qual rede estiver conectado. Se não houver perfil da rede nem da configuração do adaptador, o perfil global padrão é usado. Para atribuir um perfil a um adaptador de rede, selecione o adaptador de rede, clique em **Editar** ao lado de**Perfis atribuídos a adaptadores de rede**, selecione o perfil do menu suspenso **Perfil de firewall padrão** e clique em **Salvar**.

Quando o firewall pessoal alternar para outro perfil, uma notificação será exibida no canto inferior direito próximo ao relógio do sistema.

3.8.2.2.1 Perfis atribuídos a adaptadores de rede

Ao alternar perfis, você pode fazer rapidamente várias mudanças no comportamento do firewall. Regras personalizadas podem ser definidas e aplicadas para perfis específicos. Entradas do adaptador de rede para todos os adaptadores presentes na máquina são adicionadas automaticamente à lista de **Adaptadores de rede**.

Colunas

Nome - Nome do adaptador de rede.

Perfil de firewall padrão - O perfil padrão é usado quando a rede à qual você está conectado não tem um perfil configurado ou se o adaptador de rede estiver configurado para não usar o perfil de rede.

Perfil de rede preferido - Quando a opção **Dar preferência ao perfil de firewall da rede conectada** for ativada, o adaptador de rede usará o perfil de firewall atribuído a uma rede conectada sempre que possível.

Elementos de controle

Adicionar - Adiciona um novo adaptador de rede.

Editar - Permite editar um adaptador de rede existente.

Remover - Selecione um adaptador de rede e clique em **Remover** se quiser remover um adaptador de rede da lista.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clicar em **Cancelar** para sair sem fazer alterações.

3.8.2.3 Configuração e uso de regras

As regras representam um conjunto de condições utilizadas para testar todas as conexões de rede e todas as ações atribuídas a essas condições. Usando regras de firewall pessoal é possível definir a ação a ser feita quando diferentes tipos de conexões de rede são estabelecidos. Para acessar a configuração de filtragem de regras, navegue até **Configuração avançada** (F5) > **Firewall pessoal** > **Básico**. Algumas das regras predefinidas são vinculadas às caixas de seleção de **serviços permitidos** (Opções avançadas e IDS) e elas não podem ser desativadas diretamente; em vez disso, você pode usar essas caixas de seleção relacionadas para fazer isso.

Ao contrário da versão anterior do ESET Endpoint Security, regras são avaliadas do início para o fim. A ação da primeira regra correspondente é usada para cada conexão de rede sendo avaliada. Essa é uma alteração comportamental importante da versão anterior na qual a prioridade de regras era automática e regras mais específicas tinham prioridade superior do que as mais gerais.

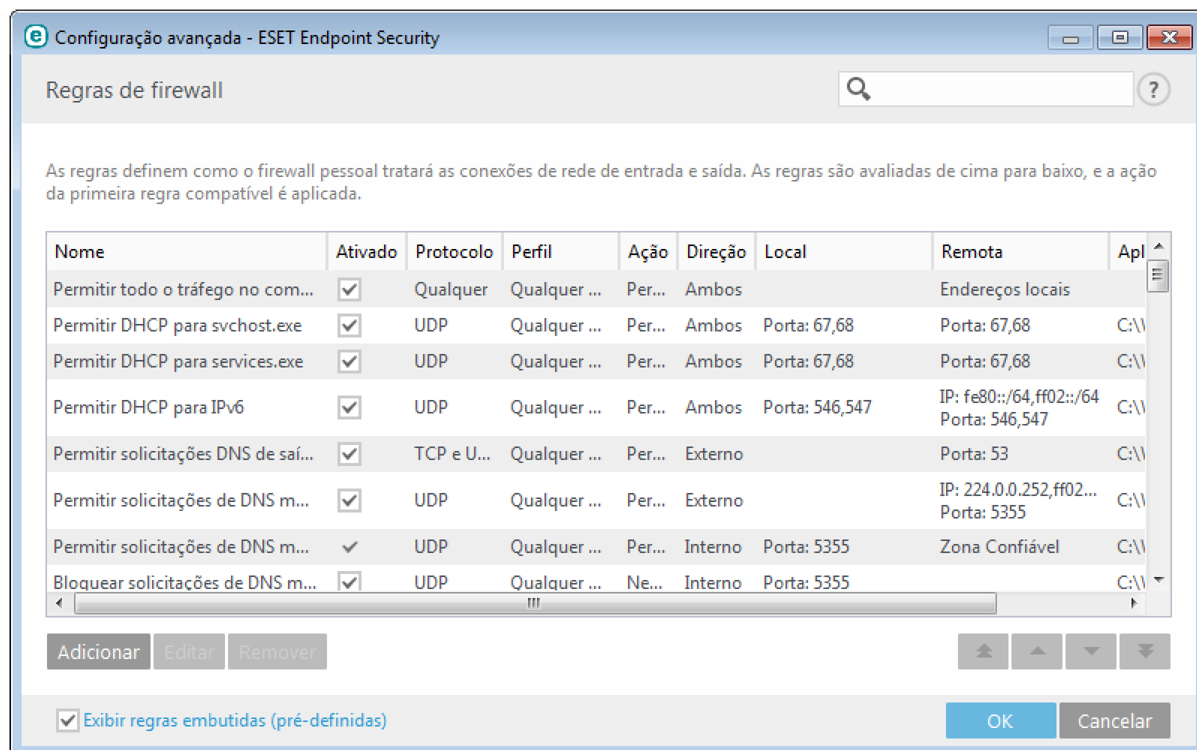
As conexões podem ser divididas em conexões de entrada e de saída. As conexões de entrada são iniciadas por um computador remoto que tenta estabelecer uma conexão com o sistema local. As conexões de saída funcionam de maneira oposta - o sistema local contata um computador remoto.

Se uma nova comunicação desconhecida for detectada, considere cuidadosamente se vai permiti-la ou negá-la. As conexões não solicitadas, não seguras ou desconhecidas representam um risco de segurança para o sistema. Se tal conexão for estabelecida, recomenda-se que seja dada atenção especial ao computador remoto e ao aplicativo tentando conectar-se ao computador. Muitas ameaças tentam obter e enviar dados particulares ou fazem download de outros aplicativos maliciosos para o computador/sistema local. O firewall pessoal permite que o usuário detecte e finalize tais conexões.

3.8.2.3.1 Regras de firewall

Clique em **Editar** ao lado de **Regras** na seção da guia **Básico** para exibir a janela **Regras de firewall**, onde a lista de todas as regras é exibida. **Adicionar**, **Editar** e **Remover** permite que você adicione, configure ou exclua regras. É possível ajustar o nível de prioridade de uma regra selecionando a regra e clicando em **Início/Para cima/Final/Para baixo**.

DICA: Você pode usar o campo **Pesquisar** para encontrar uma regra por nome, protocolo ou porta.



Colunas

Nome - Nome da regra.

Ativado - Mostra se regras estão ativadas ou desativadas, a caixa de seleção correspondente deve ser selecionada para ativar uma regra.

Protocolo - O protocolo para o qual esta regra é válida.

Perfil - Mostra o perfil de firewall para o qual esta regra é válida.

Ação - Mostra o status da comunicação (bloquear/permitir/perguntar).

Direção - Direção da comunicação (entrada/saída/ambas).

Local - Endereço IP e porta do computador local.

Remoto - Endereço IP e porta do computador remoto.

Aplicativos -O aplicativo ao qual a regra se aplica.

Elementos de controle

Adicionar -Cria uma nova regra.

Editar - Permite editar as regras existentes.

Remover - Remove as regras existentes.

Exibir regras embutidas (predefinidas) - Regras predefinidas por ESET Endpoint Security que permitem ou negam comunicações específicas. Você pode desativar essas regras, mas você não pode excluir uma regra predefinida.

Início/Para cima/Final/Para baixo- Permite que você ajuste o nível de prioridade de regras (regras são executadas

do início para o fim).

3.8.2.3.2 Trabalhando com regras

A modificação é necessária toda vez que os parâmetros monitorados são alterados. Se forem feitas alterações de forma que uma regra não preenche completamente as condições e a ação especificada não pode ser aplicada, a conexão determinada pode ser negada. Isso pode resultar em problemas com o funcionamento do aplicativo afetado por uma regra. Um exemplo é uma alteração do endereço de rede ou do número de porta para o local/ endereço remoto.

A parte superior da janela contém três guias:

- **Geral** - Especifica um nome de regra, a direção da conexão, a ação (**Permitir**, **Negar**, **Perguntar**), o protocolo e o perfil ao qual a regra se aplicará.
- **Local** - Exibe informações sobre o lado local da conexão, incluindo o número da porta local ou o intervalo de portas e o nome do aplicativo de comunicação. Também permite que você adicione uma zona pré-definida ou criada com um intervalo de endereços IP aqui, ao clicar em **Adicionar**.
- **Remoto** - Esta guia contém informações sobre a porta remota (intervalo de portas). Permite que você defina uma lista de endereços IP remotos ou zonas para uma determinada regra. Você também pode adicionar uma zona pré-definida ou criada com um intervalo de endereços IP aqui, ao clicar em **Adicionar**.

Ao criar uma nova regra, é preciso digitar o nome da regra no campo **Nome**. Selecione a direção para a qual a regra se aplica no menu suspenso **Direção** e a ação a ser executada quando um canal de comunicação encontra a regra no menu suspenso **Ação**.

Protocolo representa o protocolo de transferência usado para a regra. Selecione qual protocolo usar para determinada regra do menu suspenso.

Código/tipo ICMP representa uma mensagem ICMP identificada por um número (por exemplo, 0 representa "resposta Echo").

Por padrão, todas as regras estão ativadas para **Qualquer perfil**. Alternativamente, selecione um perfil de firewall personalizado usando o menu suspenso **Perfis**.

Se ativar o **Reportar**, a atividade conectada com a regra será registrada em um relatório. **Notificar usuário** exibe uma notificação quando a regra é aplicada.

A seguir é apresentado um exemplo no qual criamos uma nova regra para permitir que o aplicativo do navegador da Web acesse a rede. Neste exemplo, o seguinte deve ser configurado:

- Na guia **Geral**, ative a comunicação de saída por meio dos protocolos TCP e DP.
- Adicione o aplicativo do seu navegador (para o Internet Explorer, é iexplore.exe) na guia **Local**.
- Na guia **Remoto**, ative a porta número 80 se você deseja permitir navegação padrão na Internet.

OBSERVAÇÃO: Esteja ciente de que regras pré-definidas podem ser modificadas de forma limitada.

3.8.2.4 Zona confiável

A zona confiável representa um grupo de endereços de rede dos quais o Firewall pessoal permite certo tráfego de entrada usando configurações padrão. Configurações para recursos, como compartilhamento de arquivos e área de trabalho remota, na zona confiável são determinadas em opções avançadas e IDS.

A zona confiável de fato é computada dinamicamente e separadamente de cada adaptador de rede com base em qual rede o computador está conectado no momento. Endereços definidos como na zona confiável no Editor de regras são sempre confiáveis. Se um adaptador de rede estiver conectado a uma rede conhecida, então os **Endereços confiáveis adicionais** configurados para essa rede serão adicionados à zona confiável do adaptador. Se uma rede tiver o tipo de proteção Doméstica/trabalho, todas as sub-redes diretamente conectadas serão incluídas na zona confiável. A zona confiável de fato para cada adaptador de rede pode ser visualizada da janela **Configuração** em **Rede** > **Adaptadores de rede**.

OBSERVAÇÃO: A zona confiável por interface não é compatível com sistemas operacionais Windows XP. Para esses sistemas operacionais, todos os adaptadores têm a mesma zona confiável e isso também está visível na página Adaptadores de rede.

3.8.2.5 Configuração de zonas

Zonas são grupos de endereços IP, úteis quando você precisa reutilizar o mesmo conjunto de endereços em várias regras. Essas zonas podem ser configuradas em **Configuração avançada** > **Firewall pessoal** > **Básico**, clicando no botão **Editar** ao lado de **Zonas**. Para adicionar uma nova zona, clique em **Adicionar**, insira um **Nome** para a zona, uma **Descrição** e adicione um endereço IP remoto no campo **Endereço do computador remoto (IPv4/IPv6, intervalo, máscara)**.

Na janela de configuração **Zonas de firewall**, você pode especificar um nome de zona, descrição, lista de endereço de rede (consulte também Editor de redes conhecidas).

3.8.2.6 Redes conhecidas

Ao usar um computador que frequentemente se conecta a redes públicas ou redes fora de sua rede de trabalho normal, recomendamos que você verifique a credibilidade da rede de novas redes às quais está se conectando. Assim que as redes forem definidas, o ESET Endpoint Security poderá reconhecer redes confiáveis (Residencial/comercial) usando vários parâmetros de rede configurados em **Identificação da rede**. Os computadores geralmente inserem redes com endereços IP semelhantes à rede confiável. Em tais casos, o ESET Endpoint Security pode considerar uma rede desconhecida como sendo confiável (Residencial/Comercial). Recomendamos que você use a **Autenticação de rede** para evitar esse tipo de situação.

Quando um adaptador de rede é conectado a uma rede ou suas configurações de rede são reconfiguradas, o ESET Endpoint Security pesquisará na lista de rede conhecida um registro que corresponda à nova rede. Se a **Identificação da rede** e a **Autenticação da rede** (opcional) corresponderem, a rede será marcada como conectada nesta interface. Quando nenhuma rede conhecida for encontrada, uma nova rede será criada na definição da configuração da identificação de rede para identificar a rede na próxima vez que você se conectar a ela. Por padrão, a nova conexão de rede usa o tipo de proteção **pública**. A janela do diálogo **Nova conexão de rede detectada** solicitará que você escolha entre o tipo de proteção **Pública** ou **Residencial/Comercial**. Se um adaptador de rede for conectado a uma rede conhecida e essa rede for marcada como **Residencial/Comercial**, sub-redes locais do adaptador serão adicionadas à Zona confiável.

OBSERVAÇÃO: Quando você marcar **Marcar automaticamente as novas redes como públicas**, a janela do diálogo **Nova conexão de rede detectada** não aparecerá e a rede à qual você está conectado será automaticamente marcada como pública. Isso fará com que determinados recursos (por exemplo, compartilhamento de arquivos e área de trabalho remota) fiquem inacessíveis de novas redes.

Redes conhecidas podem ser configuradas manualmente na janela Editor de redes conhecidas.

3.8.2.6.1 Editor de redes conhecidas

Redes conhecidas podem ser configuradas manualmente na janela **Configuração avançada** > **Firewall pessoal** > **Redes conhecidas** clicando em **Editar**.

Colunas

Nome - Nome da rede conhecida.

Tipo de proteção - Mostra se a rede está definida como **Doméstica/Trabalho** ou **Pública**.

Perfil de firewall - Selecione o perfil no menu suspenso **Exibir regras usadas no perfil** para exibir o filtro de regras de perfis.

Elementos de controle

Adicionar - Cria uma nova rede conhecida.

Editar - Clique para editar uma rede conhecida existente.

Remover - Selecione uma rede e clique em **Remover** para removê-la da lista de redes conhecidas.

Início/Para cima/Final/Para baixo - Permite que você ajuste o nível de prioridade de redes conhecidas (redes são avaliadas do início para o fim).

Definições de configuração de rede são divididas nas seguintes guias:

Rede

Aqui você pode definir o nome de rede e selecionar o tipo de proteção (**Pública** ou **Doméstica/Trabalho**) para a rede. Use o menu suspenso **Perfil de firewall** para selecionar o perfil para esta rede. Se a rede utilizar o tipo de proteção **Doméstica/Trabalho**, todas as sub-redes de rede conectadas diretamente serão consideradas confiáveis. Por exemplo, se um adaptador de rede for conectado a esse tipo de rede com o endereço IP 192.168.1.5 e a máscara de sub-rede 255.255.255.0, a sub-rede 192.168.1.0/24 será adicionada à zona confiável desse adaptador. Se o adaptador tiver mais endereços/sub-redes, todos eles serão confiáveis, independentemente da configuração **Identificação de rede** da rede conhecida.

Além disso, endereços adicionados em **Endereços adicionais confiáveis** serão sempre adicionados à zona confiável de adaptadores conectados a essa rede (independentemente do tipo de proteção da rede).

As seguintes condições devem ser atendidas para uma rede a ser marcada como conectada na lista de redes conectadas:

- Identificação de rede - Todos os parâmetros preenchidos devem corresponder aos parâmetros de conexão ativa.
- Autenticação de rede - se o servidor de autenticação for selecionado, a autenticação bem-sucedida com o servidor de autenticação ESET deverá ocorrer.
- Restrições de rede (somente Windows XP) - todas as restrições globais selecionadas deverão ser atendidas.

Identificação da rede

A identificação da rede é executada com base nos parâmetros do adaptador da rede local. Todos os parâmetros selecionados serão comparados em relação aos parâmetros reais de conexões de redes ativas. Endereços IPv4 e IPv6 serão permitidos.

Configuração avançada - ESET Endpoint Security
Editar rede
Rede | Identificação da rede | Autenticação de rede
Quando o sufixo DNS atual for (exemplo: 'empresa.com')
hq.eset.com
Quando o endereço IP do servidor WINS for
Quando o endereço IP do servidor DNS for
Quando o endereço IP local for
Quando o endereço IP do servidor DHCP for
10.0.2.2
Quando o endereço IP do gateway for
OK Cancelar

Autenticação de rede

A autenticação de rede procura por um servidor específico na rede e usa uma criptografia assimétrica (RSA) para autenticar esse servidor. O nome da rede sendo autenticada deverá corresponder ao nome da zona definida em configurações do servidor de autenticação. O nome diferencia maiúsculas e minúsculas. Especifique um nome de servidor, uma porta de escuta do servidor e uma chave pública que corresponda à chave privada do servidor

(consulte a seção Autenticação de rede - Configuração de servidor). O nome de servidor pode ser inserido na forma de um endereço IP, DNS ou nome NetBios e pode ser seguido por um caminho especificando o local da chave no servidor (por exemplo, server_name_/directory1/directory2/authentication). Você pode especificar servidores alternativos para uso acrescentando-os ao início do caminho, separados por ponto e vírgulas.

A chave pública pode ser importada usando qualquer um dos seguintes tipos de arquivos:

- Chave pública PEM codificada (.pem), essa chave pode ser gerada usando o servidor de autenticação ESET (consulte Autenticação de rede - Configuração de servidor).
- Chave pública codificada
- Certificado de chave pública (.crt)

Clique em **Testar** para testar suas configurações. Se a autenticação foi bem sucedida, *A autenticação do servidor foi bem sucedida* será exibido. Se a autenticação não estiver configurada corretamente, será exibida uma das seguintes mensagens de erro:

Falha na autenticação do servidor. Assinatura inválida ou sem correspondência.
A assinatura de servidor não corresponde à chave pública inserida.

Falha na autenticação do servidor. O nome da rede não corresponde.
O nome da rede configurada não corresponde ao nome da zona do servidor de autenticação. Verifique ambos os nomes e certifique-se de que sejam idênticos.

Falha na autenticação do servidor. Nenhuma resposta ou resposta inválida do servidor.
Uma resposta não será recebida se o servidor não estiver em execução ou não estiver acessível. Uma resposta inválida poderá ser recebida se outro servidor HTTP estiver em execução no endereço especificado.

Chave pública inválida inserida.
Verifique se o arquivo de chave pública inserido não está corrompido.

Restrições de rede (apenas para Windows XP)

Em sistemas operacionais modernos (Windows Vista e mais recentes), cada adaptador de rede tem sua própria zona confiável e perfil de firewall ativo. Infelizmente, no Windows XP, esse layout não é compatível; portanto, todos os adaptadores de rede sempre compartilham a mesma zona confiável e perfil de firewall ativo. Isso impõe um possível risco de segurança quando a máquina estiver conectada a várias redes simultaneamente. Nesses casos, o tráfego de uma rede não confiável pode ser avaliado usando a zona confiável e o perfil de firewall configurados para a outra rede conectada. Para minimizar qualquer risco de segurança, você pode usar as restrições a seguir para evitar aplicar globalmente uma configuração de rede enquanto outra rede (possivelmente não confiável) estiver

conectada.

No Windows XP, configurações de rede conectadas (zona confiável e perfil de firewall) são aplicadas globalmente, exceto se pelo menos uma dessas restrições estiver ativada e não for atendida:

a. Apenas uma conexão ativa
b. Nenhuma conexão sem fio estabelecida
c. Nenhuma conexão insegura sem fio estabelecida

3.8.2.6.2 Autenticação de rede - Configuração de servidor

O processo de autenticação pode ser executado por qualquer computador/servidor conectado à rede que deva ser autenticado. O aplicativo Servidor de autenticação ESET precisa estar instalado em um computador/servidor que esteja sempre acessível para autenticação quando um cliente tentar se conectar à rede. O arquivo de instalação do aplicativo Servidor de autenticação ESET está disponível para download no site da ESET.

Depois de instalar o aplicativo Servidor de autenticação ESET, uma janela de diálogo será exibida (você pode acessar o aplicativo clicando em **Iniciar** > **Programas** > **ESET** > **Servidor de autenticação ESET**).

Para configurar o servidor de autenticação, insira o nome da rede de autenticação, a porta de escuta do servidor (o padrão é 80), bem como o local para armazenar o par de chaves pública e privada. Em seguida, gere as chaves pública e privada que serão utilizadas no processo de autenticação. A chave privada permanecerá no servidor, enquanto a chave pública precisará ser importada no lado do cliente na seção de autenticação da rede, ao definir uma rede na configuração do firewall.

3.8.2.7 Registro em log

O firewall pessoal do ESET Endpoint Security salva eventos importantes em um arquivo de log, que pode ser exibido diretamente no menu principal do programa. Clique em **Ferramentas** > **Arquivos de log** e então marque **Firewall pessoal** no menu suspenso **Log**. Para ativar o registro em relatório do firewall pessoal, vá para **Configuração avançada** > **Ferramentas** > **Relatórios** e defina o detalhamento mínimo de registro em relatório para **Diagnóstico.** Todas as conexões negadas serão registradas.

Os relatórios podem ser usados para detectar erros e revelar intrusos no seu sistema. Os logs da firewall pessoal da ESET contêm os seguintes dados:

- **Hora** - Data e hora do evento do evento.
- **Evento** - Nome do evento.
- **Origem** - Endereço de rede de origem.
- **Alvo** - Endereço de rede de alvo.
- **Protocolo** - Protocolo de comunicação de rede.
- **Nome da regra/worm** - Regra aplicada, ou nome do worm, se identificado.
- **Aplicativo** - Aplicativo envolvido.
- **Usuário** - Nome do usuário conectado no momento em que a infiltração foi detectada.

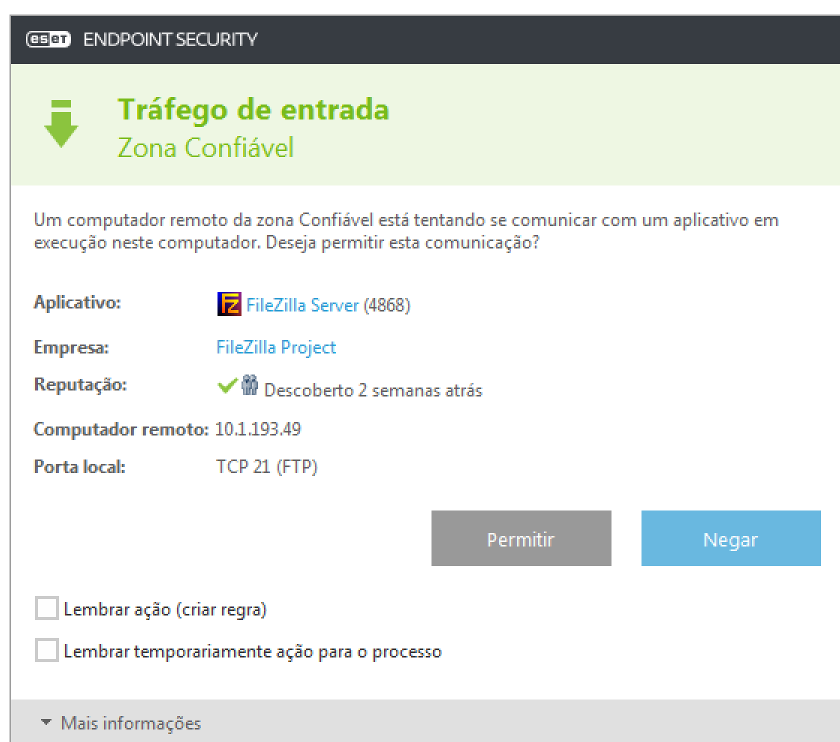
Uma análise completa desses dados pode ajudar a detectar tentativas de se comprometer a segurança do sistema. Muitos outros fatores indicam riscos de segurança potenciais e permitem que você reduza seus impactos. Alguns exemplos de possíveis indicadores de ameaças incluem conexões muito frequentes de locais desconhecidos, diversas tentativas para estabelecer conexões, aplicativos desconhecidos comunicando-se ou números de portas incomuns sendo utilizados.

3.8.2.8 Estabelecimento de uma conexão - detecção

O firewall pessoal detecta cada conexão de rede recém-criada. O modo de firewall ativo determina quais ações serão executadas para a nova conexão. Se o **Modo automático** ou o **Modo com base em políticas** estiver ativado, o firewall pessoal executará ações predefinidas sem nenhuma interação com o usuário.

O modo interativo exibe uma janela de informações que reporta a detecção de uma nova conexão de rede, suplementada com informações detalhadas sobre a conexão. O usuário pode escolher permitir a conexão ou recusá-la (bloqueio). Se houver necessidade de permitir várias vezes a mesma conexão na janela de diálogo, recomendamos que você crie uma nova regra para a conexão. Para isso, selecione a opção **Lembrar ação (criar regra)** e salve a ação como uma nova regra para o firewall pessoal. Se o firewall reconhecer a mesma conexão no futuro, ele aplicará a regra existente sem solicitar a interação do usuário.

Lembrar temporariamente ação para o processo faz com que a ação (**Permitir**/**Negar**) seja utilizada até que ocorra uma reinicialização do aplicativo, uma alteração de regras ou dos modos de filtragem ou ocorra uma atualização do módulo do Firewall ou reinicialização do sistema. Depois de qualquer uma dessas ações, as regras temporárias serão excluídas.



Tenha cuidado ao criar novas regras e permita apenas as conexões que você sabe que são seguras. Se todas as conexões forem permitidas, então o firewall pessoal falhará em realizar seu propósito. Estes são os parâmetros importantes para as conexões:

- **Lado remoto** - Somente permita conexões para endereços confiáveis e conhecidos.
- **Aplicativo local** - Não é aconselhável permitir conexões para aplicativos e processos desconhecidos.
- **Número da porta** - Em circunstâncias normais, a comunicação em portas comuns (por exemplo, o tráfego da web - porta 80) deve ser permitida.

Para se proliferar, as ameaças de computador usam frequentemente a Internet e conexões ocultas para ajudar a infectar sistemas remotos. Se as regras forem configuradas corretamente, um firewall pessoal se tornará uma ferramenta útil para a proteção contra diversos ataques de códigos maliciosos.

3.8.2.9 Resolvendo problemas com o firewall pessoal do ESET

Se você estiver tendo problemas de conectividade com o ESET Endpoint Security instalado, há várias formas de saber se o Firewall pessoal da ESET está causando o problema. Além disso, o Firewall pessoal da ESET pode ajudar você a criar novas regras ou exceções para resolver problemas de conectividade.

Consulte os seguintes tópicos para obter ajuda com a solução de problemas com o firewall pessoal da ESET:

- Assistente de solução de problemas
- Registrando e criando regras ou exceções de log
- Criando exceções de notificações do firewall
- Registro em log PCAP avançado
- Resolvendo problemas com a filtragem de protocolo

3.8.2.9.1 Assistente para solução de problemas

O assistente de solução de problemas monitora em segundo plano todas as conexões bloqueadas. Ele o orienta no processo de solução de problemas para corrigir problemas de firewall com dispositivos ou aplicativos específicos. Depois disso, ele sugere um novo conjunto de regras a serem aplicadas caso você as aprove. O **Assistente de solução de problemas** pode ser acessado no menu principal em **Configuração** > **Rede**.

3.8.2.9.2 Registrando e criando regras ou exceções de log

Por padrão, o Firewall pessoal da ESET não registra todas as conexões bloqueadas. Se você quiser ver o que foi bloqueado pelo Firewall pessoal, ative o registro em log na seção **Solução de problemas** de **Configuração avançada** em **Firewall pessoal** > **Opções avançadas e IDS**. Se você vir algo no relatório que não queira que o firewall pessoal bloqueie, poderá criar uma regra ou exceção de IDS para isso clicando com o botão direito do mouse nesse item e selecionando **Não bloquear eventos similares no futuro**. Observe que o log de todas as conexões bloqueadas pode conter milhares de itens e pode dificultar a localização de uma conexão específica nesse log. Você pode desativar o registro em log depois de resolver o problema.

Para obter mais informações sobre o log, consulte Relatórios.

Observação: use o registro em log para ver o pedido no qual o Firewall pessoal bloqueou conexões específicas. Além disso, criar regras a partir do log permite que você crie regras que façam exatamente o que você deseja.

3.8.2.9.2.1 Criar regra de log

A nova versão do ESET Endpoint Security permite que você crie uma regra do log. No menu principal, clique em **Ferramentas** > **Relatórios**. Escolha **Firewall pessoal** no menu suspenso, clique com o botão direito do mouse em sua entrada de log desejada e selecione **Não bloquear eventos similares no futuro** do menu de contexto. Uma janela de notificação exibirá sua nova regra.

Para permitir a criação de novas regras de relatório, o ESET Endpoint Security deve ser configurado com as seguintes configurações:

- define o detalhamento mínimo de registro em log como **Diagnóstico** em **Configuração avançada** (F5) > **Ferramentas** > **Relatórios**,
- ativar **Exibir notificações também para ataques sendo recebidos contra buracos de segurança** em **Configuração avançada** (F5) > **Firewall pessoal** > **IDS e opções avançadas** > **Detecção de intruso**.

3.8.2.9.3 Criando exceções de notificações do firewall pessoal

Quando o Firewall pessoal da ESET detectar atividade maliciosa na rede, uma janela de notificação descrevendo o evento será exibida. Esta notificação apresentará um link que permitirá que você saiba mais sobre o evento e configure uma exceção para ele caso queira.

OBSERVAÇÃO: se um dispositivo ou aplicativo em rede não implementar padrões de rede corretamente ele poderá acionar notificações de IDS do firewall repetidas. Você pode criar uma exceção diretamente da notificação para impedir que o Firewall pessoal da ESET detecte esse aplicativo ou dispositivo.

3.8.2.9.4 Registro em log PCAP avançado

Esse recurso tem como objetivo fornecer relatórios mais complexos para suporte ao cliente da ESET. Use esse recurso somente quando solicitado pelo suporte ao cliente da ESET, pois ele pode gerar um relatório enorme e deixar seu computador lento.

1. Vá para **Configuração avançada** > **Firewall pessoal** > **IDS e opções avançadas** > **Solução de problemas** e ative o **Ativar registro em relatório PCAP avançado**.
2. Tentativa de reproduzir o problema que você está tendo.
3. Desative o registro em log PCAP avançado.
4. O relatório PCAP pode ser encontrado no mesmo diretório no qual despejos de memória de diagnóstico são gerados:

- Microsoft Windows Vista ou mais recente

  C:\ProgramData\ESET\ESET Endpoint Segurança\Diagnostics

- Microsoft Windows XP

  C:\Documents and Settings\All Users\...

3.8.2.9.5 Resolvendo problemas com a filtragem de protocolo

Se você tiver problemas com seu navegador ou cliente de email, a primeira etapa é determinar se a filtragem de protocolo é responsável. Para fazer isso, tente desativar temporariamente a filtragem de protocolo na configuração avançada (lembre-se de ativá-la novamente depois de ter concluído; caso contrário, seu navegador e cliente de email ficarão desprotegidos). Se o problema desaparecer após desativá-la, há uma lista de problemas comuns e uma forma para resolvê-los:

Atualizar ou proteger problemas de comunicação

Se seu aplicativo avisar sobre a incapacidade de atualizar ou que um canal de comunicação não está seguro:

- Se você tiver filtragem de protocolo SSL ativada, tente desativá-la temporariamente. Se isso ajudar, você poderá continuar usando filtragem SSL e fazer o trabalho de atualização excluindo a comunicação problemática: Alterne o modo de filtragem de protocolo SSL para interativa. Execute a atualização novamente. Deve haver um diálogo informando você sobre tráfego de rede criptografado. Certifique-se de que o aplicativo corresponda ao que você está solucionando e o certificado pareça estar vindo do servidor do qual está atualizando. Em seguida, escolha lembrar a ação para esse certificado e clique em ignorar. Se não houver mais diálogos relevantes a serem exibidos, você poderá alternar o modo de filtragem de volta para automático e o problema deverá ser resolvido.
- Se o aplicativo em questão não for um navegador ou cliente de email, você poderá excluí-lo totalmente da filtragem de protocolo (fazer isso para o navegador ou cliente de email deixaria você exposto). Qualquer aplicativo que tenha tido sua comunicação filtrada anteriormente já deve estar na lista fornecida para você ao adicionar a exceção; portanto, fazer o acréscimo manualmente não deve ser necessário.

Problema ao acessar um dispositivo em sua rede

Se você não conseguir usar qualquer funcionalidade de um dispositivo em sua rede (isso poderia significar abrir uma página da Web de sua webcam ou reproduzir vídeo em um media player doméstico), tente adicionar os respectivos

IPv4 e IPv6 à lista de endereços excluídos.

Problemas com um site específico

Você pode excluir sites específicos de filtragem de protocolo usando o gerenciamento de endereços URL. Por exemplo, se você não conseguir acessar https://www.gmail.com/intl/en/mail/help/about.html, tente adicionar *gmail.com* à lista de endereços excluídos.

Erro "Alguns dos aplicativos capazes de importar o certificado raiz ainda estão em execução"

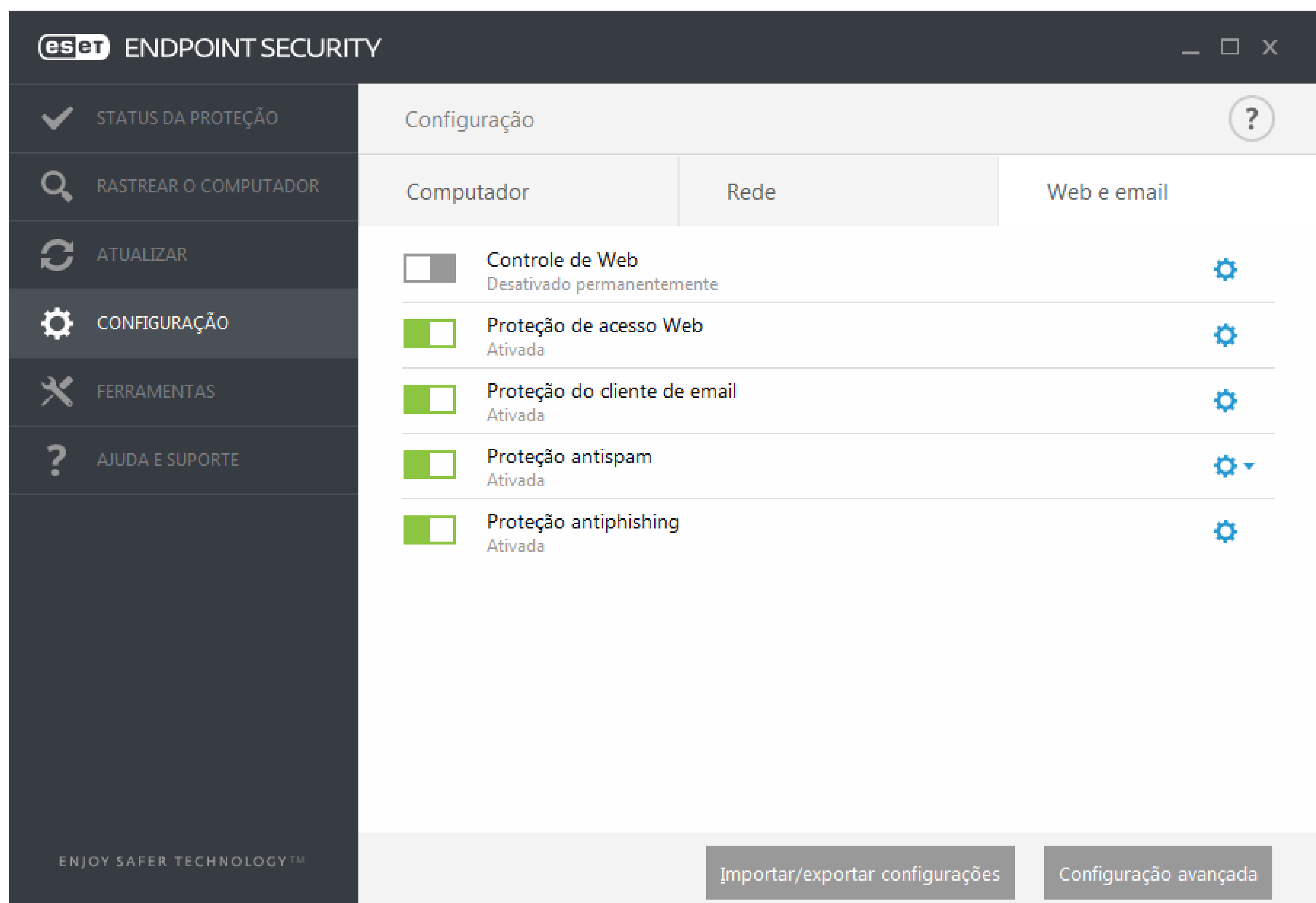
Quando você ativar a filtragem de protocolo SSL, o ESET Endpoint Security certifica-se de que aplicativos instalados confiem na forma como ele filtra protocolo SSL importando um certificado para a loja de certificados. Para alguns aplicativos, isso não é possível enquanto eles estiverem em execução. Isso inclui Firefox e Opera. Certifique-se de que nenhum deles esteja em execução (a melhor forma de fazer isso é abrir o Gerenciador de tarefas e certificar-se de que não haja firefox.exe ou opera.exe na guia Processos) e então tente novamente.

Erro sobre assinatura inválida ou emissor não confiável

Isso muito provavelmente significa que a importação descrita acima falhou. Primeiro, certifique-se de que nenhum dos aplicativos mencionados esteja em execução. Em seguida, desative a filtragem de protocolo SSL e a ative novamente. Isso executará novamente a importação.

3.8.3 Web e email

Configuração de Web e email pode ser encontrada em **Configuração** > **Web e email**. A partir daqui, você pode acessar configurações mais detalhadas do programa.



O módulo **Controle de Web** permite configurar as definições, fornecendo aos administradores ferramentas automatizadas que ajudam a proteger as estações de trabalho e a definir restrições para navegação na internet. O objetivo da funcionalidade de controle da Web é impedir o acesso a páginas com conteúdos impróprios ou prejudiciais. Para obter mais informações, consulte controle da Web.

A conectividade com a Internet é um recurso padrão em computadores pessoais. Infelizmente, ela tornou-se o meio

principal de transferência de códigos maliciosos. Por isso, é essencial refletir com atenção sobre a **Proteção do acesso à Web**.

A **Proteção do cliente de email** fornece controle da comunicação por email recebida através dos protocolos POP3 e IMAP. Usando o plug-in do cliente de email, o ESET Endpoint Security permite controlar todas as comunicações vindas através do cliente de email (POP3, IMAP, HTTP, MAPI).

A **Proteção antispam** filtra mensagens de email não solicitadas.

Quando você clicar na roda de engrenagem ao lado de **Proteção antispam**, as seguintes opções estão disponíveis:

> **Configurar...** - Abre configurações avançadas para proteção antispam de cliente de email.
>
> **Lista de permissões/proibições/exceções do usuário** - Abre uma janela de diálogo onde pode adicionar, editar ou excluir endereços de email considerados seguros ou não seguros. De acordo com as regras definidas aqui, o email desses endereços não será rastreado nem será tratado como spam. Clique em **Lista de exceções do usuário** para abrir um diálogo onde é possível adicionar, editar ou excluir endereços de email que podem ser falsos e usados para o envio de spam. As mensagens de email de endereços relacionados na Lista de exceções serão sempre rastreadas quanto a spam.

Proteção antiphishing é outra camada de proteção que fornece um nível superior de defesa de sites ilegítimos que tentam adquirir senhas e outras informações confidenciais. A Proteção antiphishing pode ser encontrada no painel **Configuração** em **Web e email**. Para obter mais informações, consulte Proteção antiphishing.

Desativar - Clique na opção para desativar a proteção de web/email/antispam para clientes de email e navegadores da Web.

3.8.3.1 Filtragem de protocolos

A proteção antivírus para os protocolos dos aplicativos é fornecida pelo mecanismo de rastreamento ThreatSense, que integra perfeitamente todas as técnicas avançadas de rastreamento de malware. A filtragem de protocolo funciona automaticamente, independentemente do navegador da Internet ou do cliente de email utilizado. Para editar configurações criptografadas (SSL), acesse **Web e email** > **SSL/TLS**.

Ativar filtragem de conteúdo do protocolo de aplicativo - Essa opção pode ser usada para desativar a filtragem de protocolo. Observe que muitos componentes do ESET Endpoint Security (Proteção do acesso à Web, Proteção de protocolos de email, Antiphishing, Controle de Web) dependem disso e não funcionarão sem ele.

Aplicativos excluídos - Permite que você exclua aplicativos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Endereços IP excluídos - Permite que você exclua endereços remotos específicos da filtragem de protocolo. Útil quando a filtragem de protocolo causar problemas de compatibilidade.

Clientes Web e email - Opção usada somente em sistemas operacionais Windows XP; permite que você selecione aplicativos dos quais todo o tráfego será filtrado por filtragem de protocolo, independentemente das portas usadas.

Registrar informações necessárias para a ESET para suporte no diagnóstico de problemas de filtragem de protocolo - Permite o registro em relatório avançado de dados de diagnóstico; use essa opção somente quando solicitado pelo suporte da ESET.

3.8.3.1.1 Clientes web e de email

OBSERVAÇÃO: Iniciando com o Windows Vista Service Pack 1 e com o Windows Server 2008, a nova arquitetura WFP (Windows Filtering Platform) é utilizada para verificar a comunicação de rede. Como a tecnologia WFP utiliza técnicas especiais de monitoramento, a seção **Clientes web e de email** não está disponível.

Devido à enorme quantidade de códigos maliciosos circulando na Internet, a navegação segura é um aspecto muito importante na proteção do computador. As vulnerabilidades do navegador da Web e os links fraudulentos ajudam o código malicioso a entrar no sistema despercebido e é por isso que o ESET Endpoint Security se focaliza na segurança do navegador da web. Cada aplicativo que acessar a rede pode ser marcado como um navegador da Internet. Aplicativos que já usaram protocolos para comunicação ou aplicativo do caminho selecionado podem ser inseridos na lista clientes de email e Web.

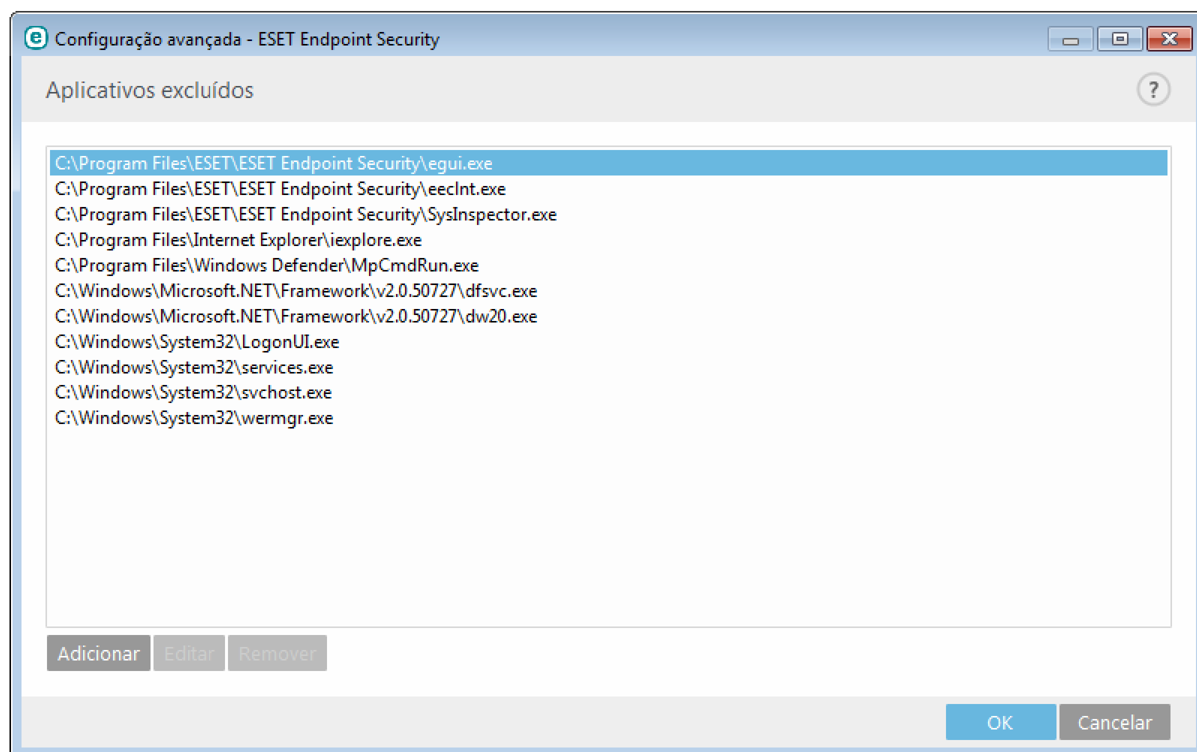
3.8.3.1.2 Aplicativos excluídos

Para excluir da filtragem de protocolos a comunicação de aplicativos específicos que possuem direito de acesso à rede, adicione-os à lista. A comunicação HTTP/POP3/IMAP dos aplicativos selecionados não será verificada quanto a ameaças. Recomendamos que você use essa técnica somente em casos em que aplicativos não funcionarem devidamente com a filtragem de protocolos ativada.

Aplicativos e serviços que já tiverem sido afetados pela filtragem de protocolos serão automaticamente exibidos depois que você clicar em **Adicionar**.

Editar - Edite as entradas selecionadas da lista.

Remover - Remove as entradas selecionadas da lista.



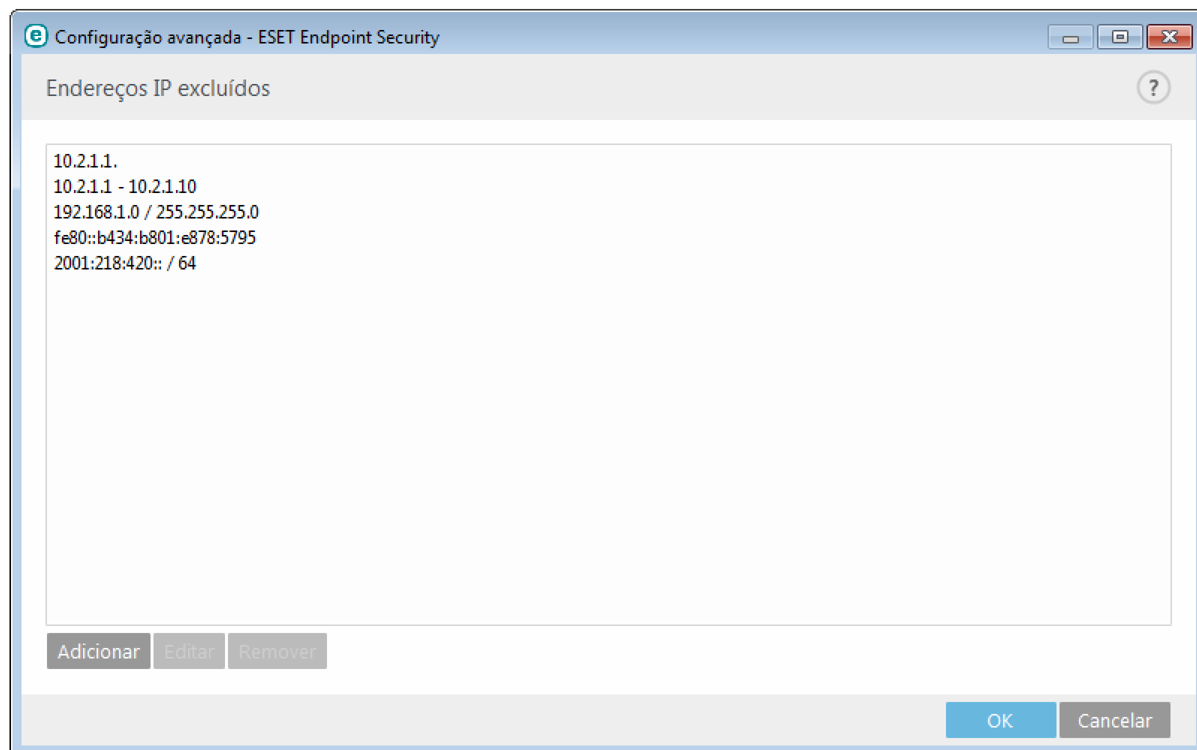
3.8.3.1.3 Endereços IP excluídos

Endereços IP nesta lista serão excluídos da filtragem de conteúdo de protocolo. A comunicação HTTP/POP3/IMAP de/para os endereços selecionados não será verificada quanto a ameaças. Recomendamos que use essa opção apenas para endereços conhecidos como sendo confiáveis.

Adicionar - Clique em adicionar um endereço IP/intervalo de endereços/sub-rede de um ponto remoto para o qual a regra é aplicada.

Editar - Edite as entradas selecionadas da lista.

Remover - Remove as entradas selecionadas da lista.



3.8.3.1.4 SSL/TLS

O ESET Endpoint Security é capaz de verificar se há ameaças em comunicações que usam o protocolo SSL. É possível usar vários modos de rastreamento para examinar comunicações protegidas por SSL com certificados confiáveis, certificados desconhecidos ou certificados excluídos da verificação das comunicações protegidas por SSL.

Ativa filtragem de protocolo SSL/TLS - Se a filtragem de protocolo estiver desativada, o programa não rastreará as comunicações em SSL.

O **Modo de filtragem de protocolo SSL/TLS** está disponível nas seguintes opções:

Modo automático - Selecione essa opção para rastrear todas as comunicações protegidas por SSL, exceto as comunicações protegidas por certificados excluídos da verificação. Se uma nova comunicação que utiliza um certificado desconhecido e assinado for estabelecida, você não será notificado e a comunicação será filtrada automaticamente. Ao acessar um servidor com um certificado não confiável marcado como confiável (ele está na lista de certificados confiáveis), a comunicação com o servidor será permitida e o conteúdo do canal de comunicação será filtrado.

Modo interativo - Se você entrar em um novo site protegido por SSL (com um certificado desconhecido), uma caixa de diálogo de seleção de ação será exibida. Esse modo permite criar uma lista de certificados SSL que serão excluídos do rastreamento.

Bloquear comunicação criptografada utilizando o protocolo obsoleto SSL v2 - A comunicação que utiliza a versão anterior do protocolo SSL será bloqueada automaticamente.

Certificado raiz

Certificado raiz - Para que a comunicação SSL funcione adequadamente nos seus navegadores/clientes de email, é fundamental que o certificado raiz da ESET seja adicionado à lista de certificados raiz conhecidos (editores). **Adicionar o certificado raiz aos navegadores conhecidos** deve estar ativado. Selecione essa opção para adicionar automaticamente o certificado raiz da ESET aos navegadores conhecidos (por exemplo, Opera e Firefox). Para navegadores que utilizam o armazenamento de certificação do sistema, o certificado será adicionado automaticamente (por exemplo, no Internet Explorer).

Para aplicar o certificado a navegadores não suportados, clique em **Exibir certificado** > **Detalhes** > **Copiar para arquivo...** e importe-o manualmente para o navegador.

Validade do certificado

Caso o certificado não possa ser verificado usando o depósito de certificados TRCA - em alguns casos, o certificado não pode ser verificado utilizando o armazenamento de Autoridades de certificação raiz confiáveis (TRCA). Isso significa que o certificado é assinado automaticamente por alguém (por exemplo, pelo administrador de um servidor Web ou uma empresa de pequeno porte) e considerar este certificado como confiável nem sempre é um risco. A maioria dos negócios de grande porte (por exemplo, bancos) usa um certificado assinado por TRCA. Se **Perguntar sobre validade do certificado** estiver selecionado (selecionado por padrão), o usuário será solicitado a selecionar uma ação a ser tomada quando for estabelecida a comunicação criptografada. Você pode selecionar **Bloquear a comunicação que utiliza o certificado** para sempre encerrar conexões criptografadas para sites com certificados não verificados.

Se o certificado não for válido ou estiver corrompido - Isso significa que o certificado expirou ou estava assinado incorretamente. Nesse caso, recomendamos que você deixe a opção **Bloquear a comunicação que utiliza o certificado** selecionada.

A **Lista de certificados conhecidos** permite que você personalize o comportamento do ESET Endpoint Security para certificados SSL específicos.

3.8.3.1.4.1 Comunicação SSL criptografada

Se seu sistema estiver configurado para usar o rastreamento de protocolo SSL, em duas situações será exibida uma janela de diálogo solicitando que você escolha uma ação:

Primeiro, se um site usar um certificado inválido ou que não possa ser verificado e o ESET Endpoint Security estiver configurado para perguntar ao usuário nesses casos (por padrão, sim para certificados que não podem ser verificados e não para inválidos), uma caixa de diálogo perguntará ao usuário se ele deseja **Permitir** ou **Bloquear** a conexão.

Depois, se o **modo de filtragem de protocolo SSL** estiver definido como **Modo interativo**, uma caixa de diálogo para cada site perguntará se você deseja **Rastrear** ou **Ignorar** o tráfego. Alguns aplicativos verificam se o tráfego SSL não foi modificado ou inspecionado por outra pessoa, sendo que em tais casos o ESET Endpoint Security deve **Ignorar** esse tráfego para manter o aplicativo funcionando.

Em ambos os casos, o usuário pode escolher lembrar a ação selecionada. Ações salvas serão armazenadas na **Lista de certificados conhecidos**.

3.8.3.1.4.2 Lista de certificados conhecidos

A **Lista de certificados conhecidos** pode ser usada para personalizar o comportamento do ESET Endpoint Security para certificados SSL específicos, bem como para lembrar ações escolhidas se o **Modo interativo** estiver selecionado no **Modo de filtragem de protocolo SSL**. A lista pode ser visualizada e editada em **Configuração avançada** (F5) > **Web e email** > **SSL/TLS** > **Lista de certificados conhecidos**.

A janela **Lista de certificados conhecidos** consiste em:

Colunas

Nome - Nome do certificado.

Emissor de certificado - Nome do autor do certificado.

Assunto do certificado - O campo de assunto identifica a entidade associada à chave pública armazenada no campo de chave pública do assunto.

Acesso - Selecione **Permitir** ou **Bloquear** como a **Ação de acesso** para permitir/bloquear a comunicação protegida por este certificado, independentemente de sua confiabilidade. Selecione **Automático** para permitir certificados confiáveis e perguntar para não confiáveis. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Rastrear - Selecione **Rastrear** ou **Ignorar** como a **Ação de rastreamento** para rastrear ou ignorar a comunicação protegida por este certificado. Selecione **Automático** para rastrear no modo automático e perguntar no modo interativo. Selecione **Perguntar** para sempre perguntar ao usuário o que fazer.

Elementos de controle

Adicionar - Um certificado pode ser carregado manualmente como um arquivo com extensão *.cer*, *.crt* ou *.pem*. Clique em Arquivo para carregar um certificado local ou clique em **URL** para especificar a localização de um certificado on-line.

Editar - Selecione o certificado que deseja configurar e clique em **Editar**.

Remover - Selecione o certificado que deseja excluir e clique em **Remover**.

OK/Cancelar - Clique em **OK** se quiser salvar alterações ou clicar em **Cancelar** para sair sem salvar.

3.8.3.2 Proteção do cliente de email

3.8.3.2.1 Clientes de email

A integração do ESET Endpoint Security com os clientes de email aumenta o nível de proteção ativa contra códigos maliciosos nas mensagens de email. Se o seu cliente de email for compatível, essa integração poderá ser ativada no ESET Endpoint Security. Quando a integração for ativada, a barra de ferramentas do ESET Endpoint Security será inserida diretamente no cliente de email (a barra de ferramentas para versões mais recentes do Windows Live Mail não é inserida), permitindo proteção mais eficiente aos emails. As configurações de integração estão localizadas em **Configuração** > **Configuração avançada** > **Web e email** > **Proteção do cliente de email** > **Clientes de email**.

Integração com clientes de email

Os clientes de email atualmente suportados incluem o Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail. A proteção de email funciona como um plug-in para esses programas. A principal vantagem do plug-in é que ele não depende do protocolo usado. Quando o cliente de email recebe uma mensagem criptografada, ela é descriptografada e enviada para o scanner de vírus. Para obter uma lista completa dos clientes de email suportados e suas versões, consulte o seguinte artigo da Base de conhecimento da ESET.

Mesmo se a integração não estiver ativada, as comunicações por email ainda estarão protegidas pelo módulo de proteção do cliente de email (POP3, IMAP).

Ative a opção **Desativar verificação de alteração na caixa de entrada** se houver redução na velocidade do sistema ao trabalhar com o seu cliente de email (somente para MS Outlook). Essa situação pode ocorrer ao recuperar emails do

Kerio Outlook Connector Store.

Email para ser rastreado

Email recebido - Alterna a verificação das mensagens recebidas.
Email enviado - Alterna a verificação das mensagens enviadas.
Email lido - Alterna a verificação das mensagens lidas.

Ação que será executada no email infectado

Nenhuma ação - Se ativada, o programa identificará anexos infectados, mas não será tomada qualquer ação em relação aos emails.
Excluir email - O programa notificará o usuário sobre infiltrações e excluirá a mensagem.
Mover email para a pasta Itens excluídos - Os emails infectados serão movidos automaticamente para a pasta Itens excluídos.
Mover email para a pasta - Os emails infectados serão movidos automaticamente para a pasta especificada.

Pasta - Especifique a pasta personalizada para a qual você deseja mover os emails infectados quando detectados.

Repetir o rastreamento após atualização - Alterna o rastreamento depois de uma atualização do banco de dados da assinatura de vírus.

Aceitar resultados de rastreamento de outros módulos - Se essa opção for selecionada, o módulo de proteção do email aceitará os resultados de rastreamento de outros módulos de proteção (rastreamento de aplicativos POP3, IMAP).

3.8.3.2.2 Protocolos de email

Os protocolos IMAP e POP3 são os protocolos mais amplamente utilizados para receber comunicação em um aplicativo cliente de email. O ESET Endpoint Security fornece proteção para estes protocolos, independentemente do cliente de email usado, sem necessidade de reconfiguração do cliente de email.

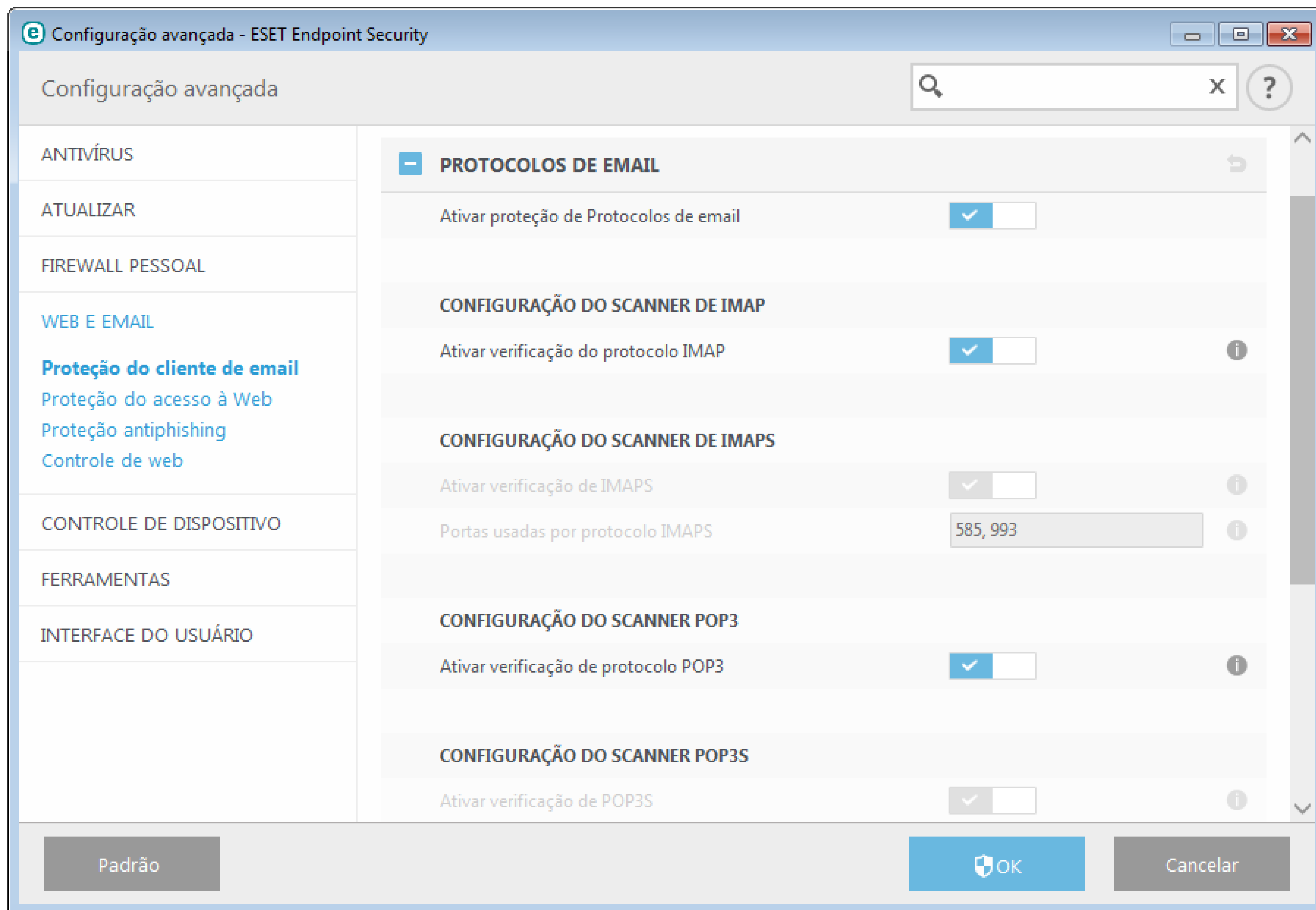
Você pode configurar a verificação de protocolos IMAP/IMAPS e POP3/POP3S na Configuração avançada. Para acessar essa configuração, expanda **Web e email** > **Proteção do cliente de email** > **Protocolos de email**.

Ativar proteção de protocolos de email - Ativa a verificação de protocolos de email.

No Windows Vista e em versões posteriores, os protocolos IMAP e POP3 são automaticamente detectados e rastreados em todas as portas. No Windows XP, somente as **Portas usadas pelo protocolo IMAP/POP3** configuradas serão rastreadas para todos os aplicativos, assim como todas as portas serão rastreadas para aplicativos marcados como Clientes web e email.

O ESET Endpoint Security também é compatível com o rastreamento de protocolos IMAPS e POP3S, que utilizam um canal criptografado para transferir as informações entre servidor e cliente. O ESET Endpoint Security verifica as comunicações utilizando os protocolos SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). O programa rastreará somente tráfego em portas definidas em **Portas usadas pelo protocolo IMAPS/POP3S**, independentemente da versão do sistema operacional.

Comunicações criptografadas não serão rastreadas quando as configurações padrão estiverem em uso. Para ativar o rastreamento da comunicação criptografada, acesse SSL/TLS em Configuração avançada, clique em **Web e email** > **SSL/TLS** e selecione **Ativar filtragem de protocolo SSL**.



3.8.3.2.3 Alertas e notificações

A proteção de email fornece controle da comunicação por email recebida pelos protocolos POP3 e IMAP. Usando o plug-in para Microsoft Outlook e outros clientes de email, o ESET Endpoint Security permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP). Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado inclusos no mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com a base de dados de assinaturas de vírus. O rastreamento das comunicações por protocolos POP3 e IMAP é independente do cliente de email usado.

As opções dessa funcionalidade estão disponíveis em **Configuração avançada** em **Web e email** > **Proteção do cliente de email** > **Alertas e notificações**.

Configuração dos parâmetros do mecanismo ThreatSense - A configuração avançada do scanner de vírus permite configurar alvos do rastreamento, métodos de detecção, etc. Clique para exibir a janela de configuração do scanner de vírus detalhada.

Depois que um email tiver sido verificado, uma notificação com o resultado da verificação pode ser anexada à mensagem. É possível selecionar **Acrescentar mensagem de marca nos emails recebidos e lidos, Acrescentar observação ao assunto de email infectado recebido e lido** ou **Acrescentar mensagens de marca a email enviado**. Esteja ciente que em algumas ocasiões mensagens de marca podem ser omitidas em mensagens HTML problemáticas ou se mensagem forem forjadas por malware. As mensagens de marca podem ser adicionadas a um email recebido e lido ou a um email enviado, ou ambos. As opções disponíveis são:

- **Nunca** - nenhuma mensagem de marca será adicionada.
- **Somente para email infectado** - Somente mensagens contendo software malicioso serão marcadas como rastreadas (padrão).
- **Para todos os emails rastreados** - o programa anexará mensagens a todos os emails rastreados.

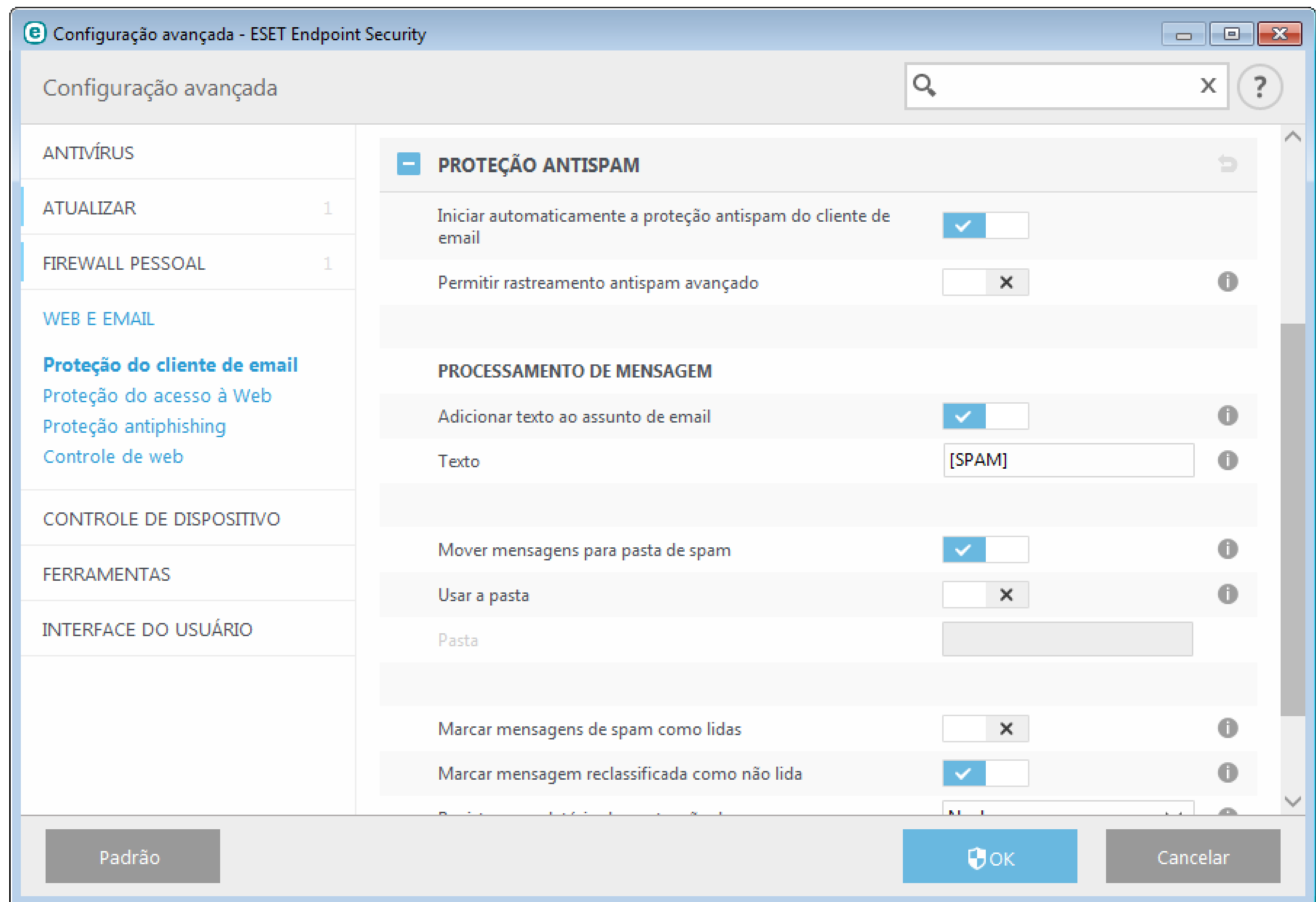
Acrescentar observação ao assunto de email infectado enviado - Desative essa opção se você quiser que a proteção de email inclua um alerta de vírus no assunto de um email infectado. Esse recurso permite a filtragem simples com base em assunto de email infectado (se compatível com o seu programa de email). Esse recurso aumenta o nível de

credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

Modelo adicionado ao assunto de email infectado - Edite esse modelo se desejar modificar o formato de prefixo do assunto de um email infectado. Essa função substituirá o assunto da mensagem *"Olá"* com o prefixo *"[vírus]"* para o seguinte formato: *"[virus] Olá"*. A variável *%VIRUSNAME%* representa a ameaça detectada.

3.8.3.2.4 Proteção antispam

Os emails não solicitados, conhecidos como spams, estão entre os maiores problemas da comunicação eletrônica. Os spams representam até 80 por cento de toda a comunicação por email. A proteção Antispam serve para proteger contra esse problema. Combinando diversos princípios de segurança de email, o módulo Antispam fornece filtragem superior para manter a caixa de entrada limpa.



Um princípio importante para a detecção do spam é a capacidade de reconhecer emails não solicitados com base em endereços confiáveis predefinidos (lista de permissões) e em endereços de spam (lista de proibições). Todos os endereços de sua lista de contatos são automaticamente acrescentados à lista de permissões, bem como todos os demais endereços marcados pelo usuário como seguros.

O principal método usado para detectar spam é o rastreamento das propriedades da mensagem de email. As mensagens recebidas são verificadas quanto aos critérios Antispam básicos (definições da mensagem, heurísticas estatísticas, reconhecimento de algoritmos e outros métodos únicos) e o valor do índice resultante determina se uma mensagem é spam ou não.

Iniciar automaticamente a proteção antispam do cliente de email - Quando ativada, a proteção antispam será ativada automaticamente na inicialização do sistema.

Permitir rastreamento antispam avançado - Dados antispam adicionais serão baixados periodicamente, aumentando as capacidades antispam e produzindo melhores resultados.

A proteção antispam no ESET Endpoint Security permite definir diferentes parâmetros para trabalhar com as listas de emails. As opções são:

Processamento de mensagens

Adicionar texto ao assunto de email - Permite adicionar uma cadeia de caracteres de prefixo personalizado à linha de assunto das mensagens classificadas como spam. O padrão é "[SPAM]".

Mover mensagens para pasta spam - Quando ativada, as mensagens de spam serão movidas para a pasta padrão de lixo eletrônico e as mensagens reclassificadas como não spam serão movidas para a caixa de entrada. Ao clicar com o botão direito em uma mensagem de email e selecionar ESET Endpoint Security no menu de contexto, é possível escolher das opções aplicáveis.

Usar a pasta - Esta opção move o spam para uma pasta definida pelo usuário.

Marcar mensagens de spam como lidas - Selecione isto para marcar automaticamente spam como lido. Isso o ajudará a concentrar sua atenção em mensagens "limpas".

Marcar mensagens reclassificadas como não lidas - As mensagens originariamente classificadas como spam, mas posteriormente marcadas como "limpas" serão exibidas como não lidas.

Registro em log da pontuação de spam - O mecanismo antispam do ESET Endpoint Security atribui uma pontuação de spam a cada mensagem rastreada. A mensagem será registrada no log de antispam (**ESET Endpoint Security** > **Ferramentas** > **Arquivos de log** > **Proteção antispam**).

- **Nenhum** - A pontuação do rastreamento antispam não será registrada.
- **Reclassificado e marcado como spam** - Selecione isto se desejar registrar uma pontuação de spam para mensagens marcadas como SPAM.
- **Todas** - Todas as mensagens serão registradas no log com a pontuação de spam.

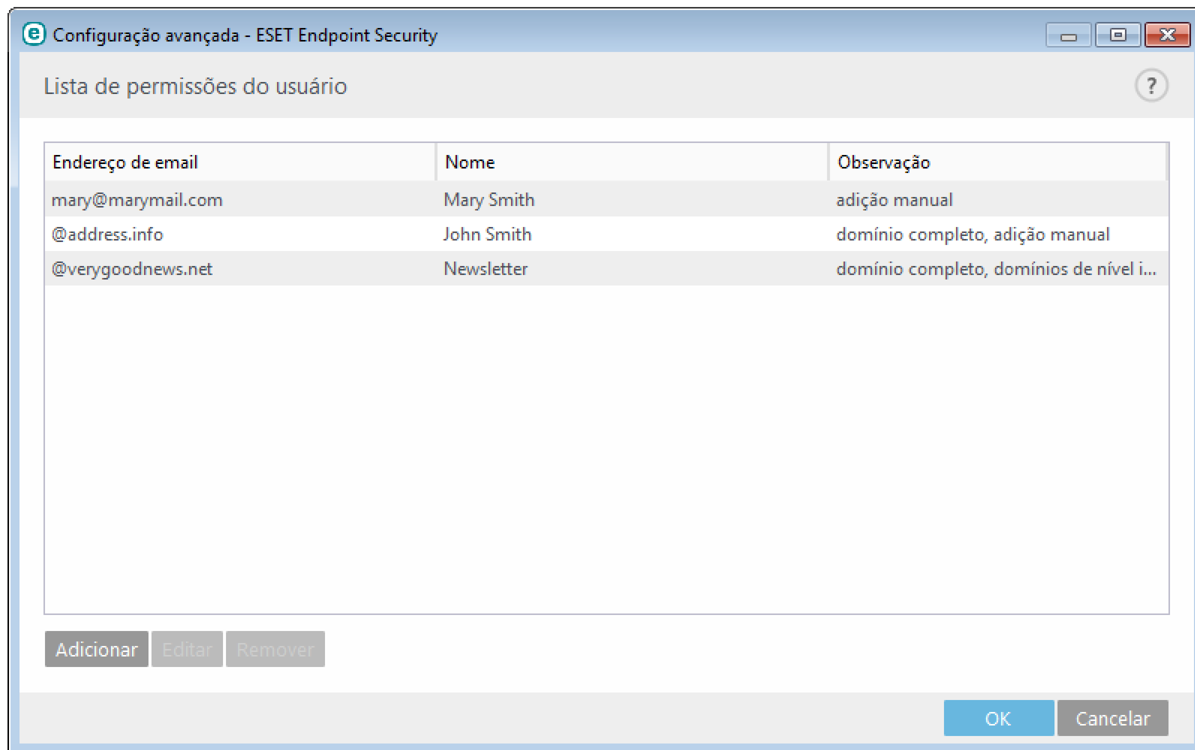
OBSERVAÇÃO: Ao clicar em uma mensagem na pasta de email spam, é possível selecionar **Reclassificar mensagens selecionadas como NÃO spam** e a mensagem será movida para a caixa de entrada. Ao clicar em uma mensagem que você considera ser spam na caixa de entrada, selecione **Reclassificar mensagens como spam** e a mensagem será movida para a pasta de spam. Você pode selecionar várias mensagens e realizar a ação em todas elas ao mesmo tempo.

OBSERVAÇÃO: o ESET Endpoint Security é compatível com a proteção antispam para Microsoft Outlook, Outlook Express, Windows Mail e Windows Live Mail.

3.8.3.2.4.1 Lista de proibições/Lista de permissões/Lista de exceções

Para fornecer proteção contra emails não solicitados, o ESET Endpoint Security permite classificar endereços de email usando listas especializadas. A lista de permissões contém endereços de email seguros. As mensagens de usuários na lista de permissões estão sempre disponíveis na pasta de email de entrada. A lista de proibições contém endereços de email classificados como spam, e todas as mensagens de remetentes na lista de proibições são marcadas de acordo. A lista de exceções contém endereços de email que são sempre verificados quanto a spam, mas também pode conter endereços de mensagens de email não solicitadas que podem não ser reconhecidas como spam inicialmente.

Todas as listas podem ser editadas da janela do programa principal do ESET Endpoint Security em **Configuração avançada** > **Web e email** > **Proteção do cliente de email** > **Catálogos de endereços antispam** usando os botões Adicionar, Editar e Remover em cada janela de diálogo da lista ou de **Configuração** > **Web e email** depois que você clicar na roda de engrenagem ao lado de **Proteção antispam**.



Por padrão, o ESET Endpoint Security adiciona à lista de permissões todos os endereços do catálogo de endereços de clientes de email compatíveis. Por padrão, a lista de proibições está vazia. Por padrão, a lista de exceções relaciona apenas os endereços de email do próprio usuário.

3.8.3.2.4.2 Adição de endereços à lista de permissões e à lista de proibições

Emails de pessoas com quem você se comunica com frequência podem ser adicionados à lista de permissões para garantir que nenhuma mensagem desses remetentes permitidos seja classificada como spam. Endereços de spam conhecidos podem ser adicionados à lista de proibições e sempre podem ser classificados como spam. Para adicionar um novo endereço à lista de permissões ou de proibições, clique com o botão direito do mouse no email e selecione **ESET Endpoint Security** > **Adicionar à lista de permissões** ou **Adicionar à lista de proibições**, ou clique no botão **Endereço confiável** ou **Endereço de spam** na barra de ferramentas antispam do ESET Endpoint Security, em seu cliente de email.

Esse processo também se aplica aos endereços de spam. Se um endereço de email for listado na lista de proibições, cada mensagem de email enviada daquele endereço será classificada como spam.

3.8.3.2.4.3 Marcando mensagens como spam ou não spam

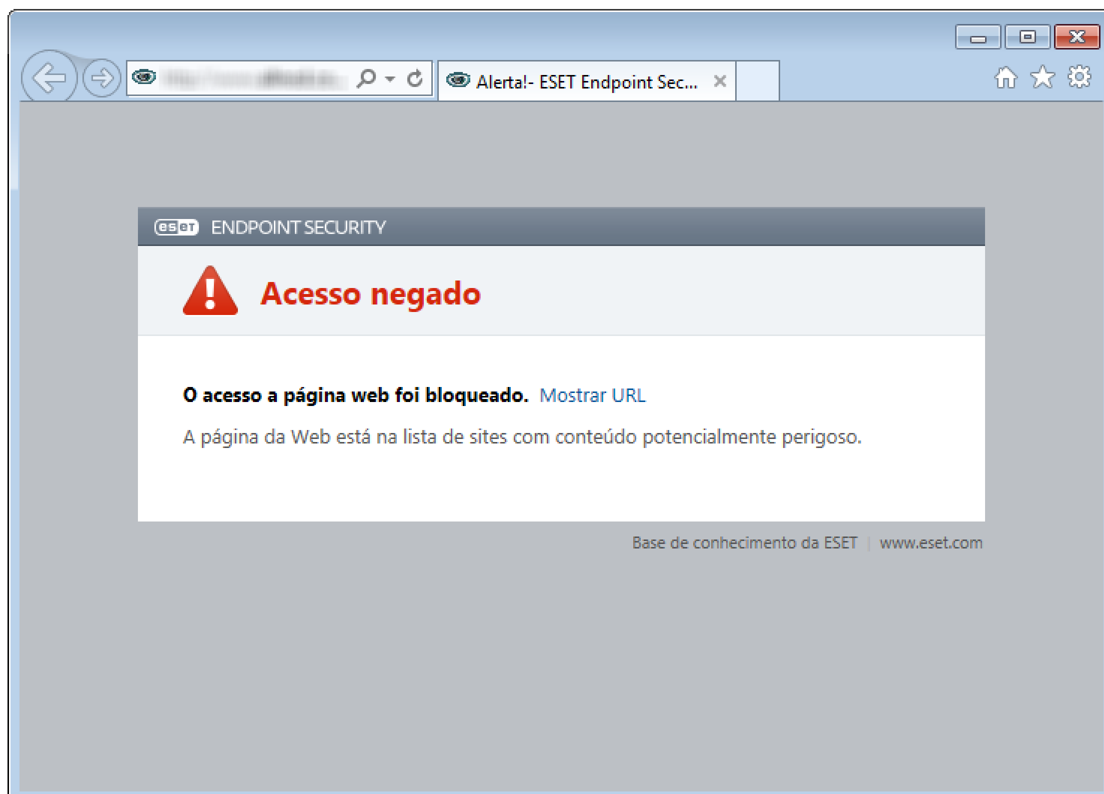
Qualquer mensagem exibida em seu cliente de email pode ser marcada como spam. Para isso, clique com o botão direito do mouse na mensagem e clique em **ESET Endpoint Security** > **Reclassificar mensagens selecionadas como spam** ou clique em **Spam** na barra de ferramentas antispam do ESET Endpoint Security localizada na seção superior de seu cliente de email.

As mensagens reclassificadas são automaticamente movidas para a pasta SPAM, mas o endereço de email do remetente não é acrescentado à **Lista de proibições**. De modo similar, as mensagens podem ser classificadas como “não spam” clicando em **ESET Endpoint Security** > **Reclassificar mensagens selecionadas como não spam** ou em **Não spam** na barra de ferramentas antispam do ESET Endpoint Security localizada na seção superior de seu cliente de email. Se as mensagens da pasta **Lixo eletrônico** forem classificadas como não spam, elas serão movidas para a sua **Caixa de entrada**. Marcar uma mensagem como não spam acrescenta automaticamente o endereço do remetente à **Lista de permissões**.

3.8.3.3 Proteção do acesso à Web

A conectividade com a Internet é um recurso padrão na maioria de computadores pessoais. Infelizmente, ela tornou-se o meio principal de transferência de códigos maliciosos. A proteção de acesso à Web funciona ao monitorar a comunicação entre os navegadores da web e servidores remotos e cumpre as regras do protocolo HTTP (Hypertext Transfer Protocol) e HTTPS (comunicação criptografada).

O acesso à páginas da Web conhecidas como tendo conteúdo malicioso é bloqueado antes que o conteúdo seja baixado. Todas as outras páginas da Web serão rastreadas pelo mecanismo de rastreamento ThreatSense quando forem carregadas e bloqueadas se conteúdo malicioso for detectado. A proteção do acesso à Web oferece dois níveis de proteção, bloqueio por lista de proibições e bloqueio por conteúdo.



Recomendamos enfaticamente que você mantenha a proteção de acesso à Web ativada. Essa opção pode ser acessada a partir da janela do programa principal do ESET Endpoint Security localizada em **Configuração** > **Web e email** > **Proteção de acesso à Web**.

As seguintes opções estão disponíveis em **Configuração avançada** (F5) > **Web e email** > **Proteção de acesso à Web**:

- **Protocolos da Web** - Permite que você configure o monitoramento para esses protocolos padrão, que são usados pela maioria dos navegadores de Internet.
- **Gerenciamento de endereços URL** - Permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação.
- **Configuração de parâmetros do mecanismo ThreatSense** - Configuração avançada do rastreador de vírus - permite definir as configurações, como tipos de objetos para rastreamento (emails, arquivos, etc.), métodos de detecção para proteção de acesso à Web, etc.

3.8.3.3.1 Protocolos da web

Por padrão, o ESET Endpoint Security é configurado para monitorar o protocolo HTTP usado pela maioria dos navegadores de Internet.

No Windows Vista e versões posteriores, o tráfego HTTP é sempre monitorado em todas as portas para todos os aplicativos. No Windows XP, é possível modificar as **Portas utilizadas pelo protocolo HTTP** em **Configuração avançada** (F5) > **Web e email** > **Proteção do acesso à Web** > **Protocolos da Web** > **Configuração do rastreamento HTTP**. O tráfego HTTP é monitorado nas portas especificadas para todos os aplicativos e em todas as portas para aplicativos marcados como Clientes Web e email.

O ESET Endpoint Security também oferece suporte à verificação do protocolo HTTPS. A comunicação HTTPS utiliza um canal criptografado para transferir as informações entre servidor e cliente. O ESET Endpoint Security verifica as comunicações utilizando os protocolos SSL (Camada de soquete seguro) e TLS (Segurança da camada de transporte). O programa rastreará somente tráfego em portas definidas em **Portas usadas pelo protocolo HTTPS**, independentemente da versão do sistema operacional.

Comunicações criptografadas não serão rastreadas quando as configurações padrão estiverem em uso. Para ativar o rastreamento da comunicação criptografada, acesse SSL/TLS em Configuração avançada, clique em **Web e email** > **SSL/TLS** e selecione **Ativar filtragem de protocolo SSL**.

3.8.3.3.2 Gerenciamento de endereços URL

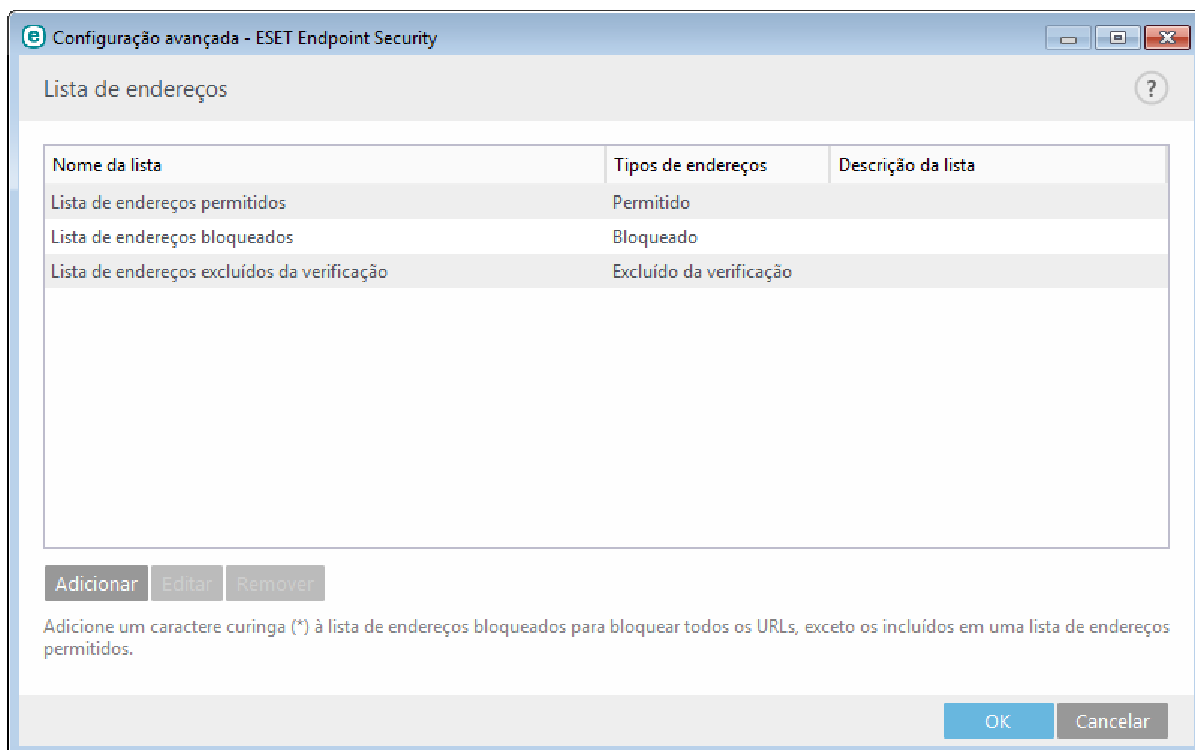
O gerenciamento de endereços URL permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação.

Sites na **Lista de endereços bloqueados** não estarão acessíveis, exceto se também forem incluídos na **Lista de endereços permitidos**. Sites na **Lista de endereços excluídos da verificação** não serão rastreados quanto a código malicioso quando acessados.

A opção **Ativar filtragem de protocolo SSL/TLS** deve ser selecionada se você quiser filtrar endereços HTTPS além de páginas HTTP. Caso contrário, somente os domínios de sites HTTPS que você tenha visitado serão adicionados, não a URL completa.

Em todas as listas, os símbolos especiais * (asterisco) e ? (ponto de interrogação) podem ser usados. O asterisco representa qualquer número ou caractere, enquanto o ponto de interrogação representa qualquer caractere. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter apenas os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista. Consulte Adicionar endereço HTTP/máscara de domínio para saber como combinar com segurança um domínio completo, incluindo todos os subdomínios. Para ativar uma lista, ative a opção **Lista ativa**. Se você desejar ser notificado ao inserir um endereço da lista atual, ative **Notificar ao aplicar**.

Se você quiser bloquear todos os endereços HTTP, exceto endereços presentes na **Lista de endereços permitidos** ativa, adicione * à **Lista de endereços bloqueados** ativa.



Adicionar - Crie uma nova lista além das predefinidas. Isso pode ser útil se você quiser dividir logicamente diferentes grupos de endereços. Por exemplo, uma lista de endereços bloqueados pode conter endereços de alguma lista pública externa de proibições e uma segunda pode conter sua própria lista de proibições, que facilita a atualização da lista externa enquanto mantém a sua intacta.

Editar - Modifica listas existentes. Use isso para adicionar ou remover endereços das listas.

Remover - Exclui a lista existente. Possível somente para listas criadas com **Adicionar**, não para as padrão.

3.8.3.4 Proteção antiphishing

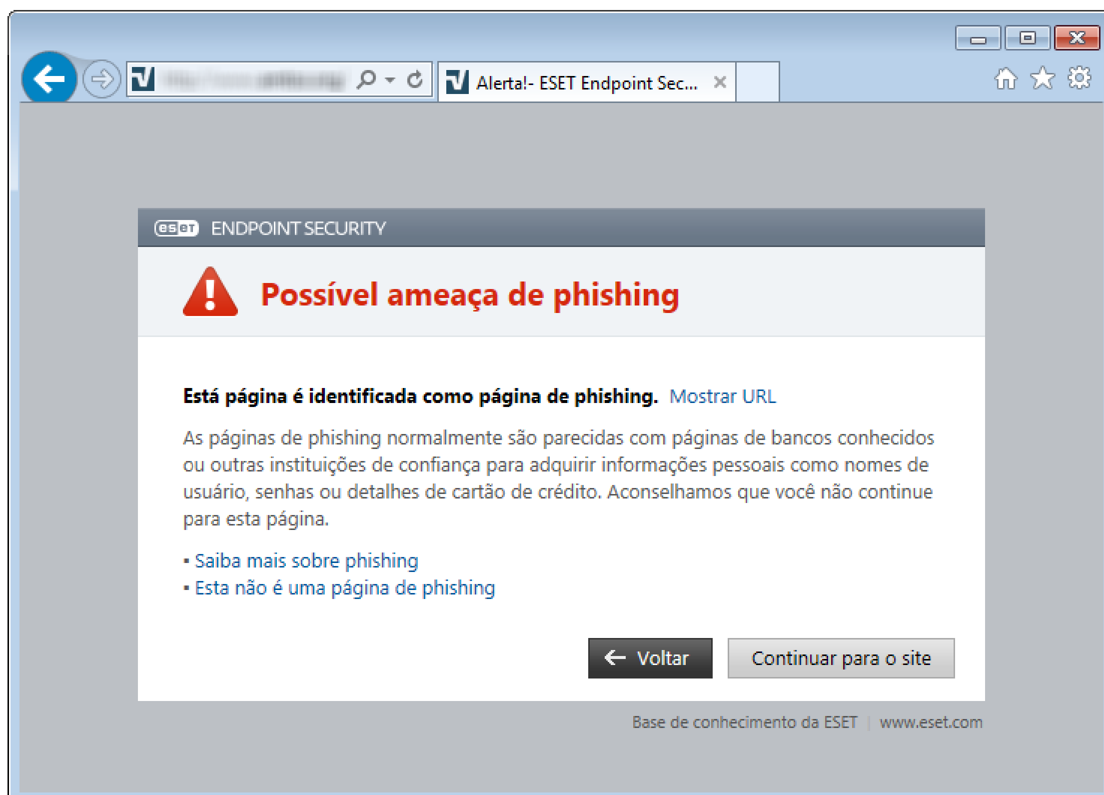
O termo roubo de identidade define uma atividade criminal que usa engenharia social (a manipulação de usuários para obter informações confidenciais). O roubo de identidade é frequentemente usado para obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN e outros. Leia mais sobre essa atividade no glossário. O ESET Endpoint Security oferece proteção antiphishing; páginas da web conhecidas por distribuir esse tipo de conteúdo podem ser bloqueadas.

Recomendamos que você ative a proteção antiphishing no ESET Endpoint Security. Para isso, abra a **Configuração avançada** (F5) e vá para **Web e email** > **Proteção antiphishing**.

Visite nosso artigo da Base de conhecimento para mais informações sobre a Proteção antiphishing no ESET Endpoint Security.

Acessando um site de roubo de identidade

Ao acessar um site de roubo de identidade reconhecido, você verá a caixa de diálogo a seguir no seu navegador da web. Se ainda quiser ter acesso ao site, clique em **Continuar para o site** (não recomendável).



OBSERVAÇÃO: por padrão, sites de roubo de identidade em potencial que tiverem sido permitidos expirarão horas depois. Para permitir um site permanentemente, use a ferramenta de gerenciamento de endereços de URL. A partir de **Configuração avançada** (F5) abra **Web e email** > **Proteção do acesso à Web** > **Gerenciamento de endereços URL** > **Lista de endereços**, clique em **Editar** e adicione o site que deseja editar na lista.

Denúncia de site de roubo de identidade

O link Denunciar permite que você denuncie um site de phishing/malicioso para análise da ESET.

OBSERVAÇÃO: antes de enviar um site para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:

- o site não foi detectado,
- o site foi detectado incorretamente como uma ameaça. Nesse caso, é possível relatar um site de phishing falso positivo.

Como alternativa, você pode enviar o site por email. Envie seu email para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o site (por exemplo, o site do qual você foi enviado, como ouviu falar sobre ele, etc.).

3.8.4 Controle de web

A seção Controle de Web permite que você defina as configurações que protegem sua empresa do risco de responsabilidade legal. O Controle de Web pode regulamentar o acesso a sites que violem direitos de propriedade intelectual. O objetivo é impedir que os funcionários acessem páginas com conteúdo inadequado ou prejudicial, ou páginas que possam ter impacto negativo sobre a produtividade.

O Controle de Web permite bloquear sites que possam conter material potencialmente ofensivo. Além disso, os empregadores ou administrador do sistema podem proibir o acesso para mais de 27 categorias de site predefinidas e mais de 140 subcategorias.

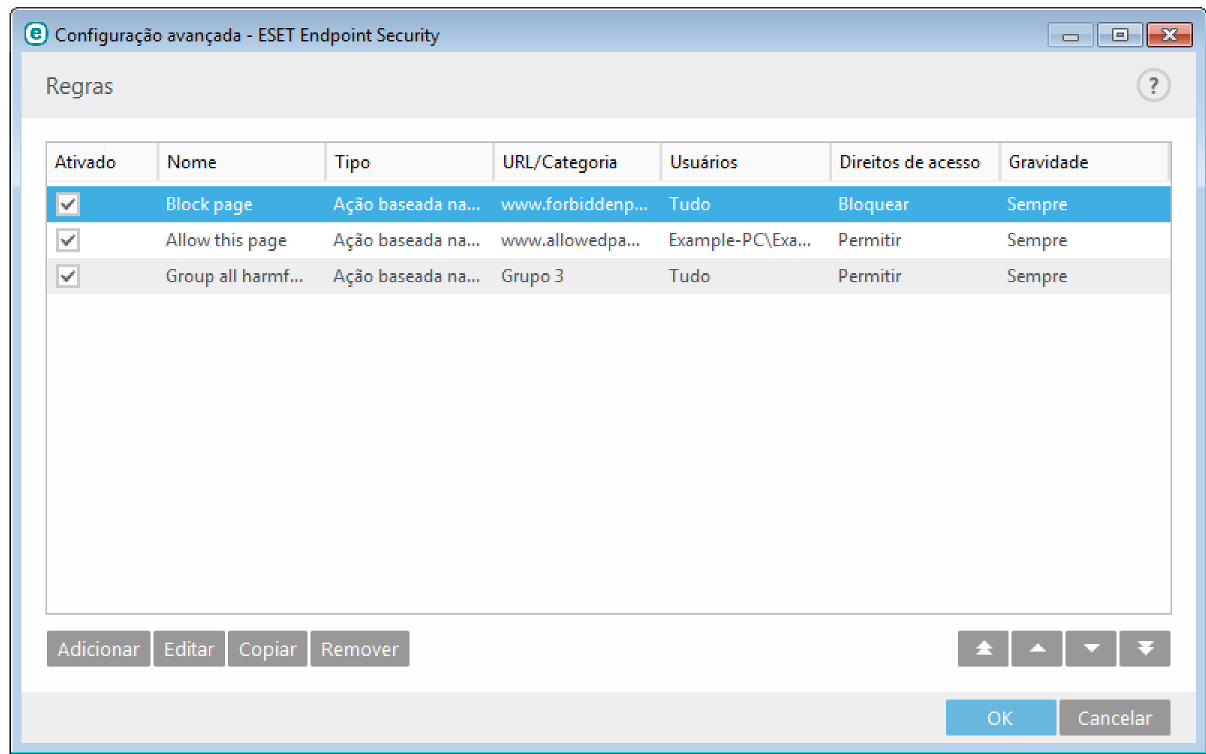
Por padrão, o controle da Web está desativado. Para ativar o Controle de Web, pressione F5 para acessar a **Configuração avançada** e expanda **Web e email** > **Controle de Web**. Selecione **Integrar ao sistema** para ativar o controle da Web no ESET Endpoint Security. Clique em **Editar** ao lado de **Regras** para acessar a janela do Editor de regras do Controle de Web.

Os campos **Mensagem de página da web bloqueada** e **Gráfico de página da web bloqueada** permitem que você personalize a mensagem exibida quando um site for bloqueado.

DICA: Um exemplo de mensagem de página da web bloqueada seria *A página da web foi bloqueada porque ela é considerada com conteúdo inadequado ou prejudicial. Entre em contato com seu administrador para mais detalhes,* e é possível inserir um endereço web ou caminho de rede com uma imagem personalizada, por exemplo *http://test.com/test.jpg*. O tamanho de imagem personalizado é definido automaticamente como 90 x 30, as imagens serão redimensionadas automaticamente para este tamanho se não estiverem nele.

3.8.4.1 Regras

A janela do editor de **Regras** exibe regras existentes com base em URL ou com base em categoria.



A lista de regras contém diversas descrições de uma regra, tais como nome, tipo de bloqueio, ação a ser realizada após a correspondência de uma regra de controle da Web e a gravidade do relatório.

Clique em **Adicionar** ou **Editar** para gerenciar uma regra. Clique em **Copiar** para criar uma nova regra com opções predefinidas usadas para outra regra selecionada. Ao pressionar **Ctrl** e clicar, você pode selecionar várias regras e excluir todas as regras selecionadas. A caixa de seleção **Ativado** desativará ou ativará uma regra; isso pode ser útil caso não deseje excluir uma regra permanentemente se você pretende usá-la no futuro.

As regras são classificadas na ordem determinando sua prioridade, com as regras de prioridade superior no início. A avaliação de regras com base em URL sempre tem prioridade superior do que a avaliação com base em categoria. Por exemplo, se uma regra com base em URL estiver sob uma regra com base em categoria na lista de regras, a regra com base em URL terá prioridade superior e será avaliada primeiro.

3.8.4.1.1 Adicionar regras de controle de web

A janela Regras de controle da Web permite criar ou modificar manualmente uma regra de filtro do controle da Web existente.

Insira uma descrição da regra no campo **Nome** para melhor identificação. Clique na opção **Ativado** para ativar ou desativar esta regra. Isso pode ser útil caso não deseje excluir a regra permanentemente.

Tipo de ação

- **Ação baseada na URL** - Para regras que controlam acesso a um determinado site, insira a URL no campo **URL**.
- **Ação baseada na categoria** - Quando isto estiver selecionado, defina a categoria para sua ação usando o menu suspenso.

Os símbolos especiais * (asterisco) e ? (ponto de interrogação) não podem ser usados na lista de endereços de URL. Ao criar um grupo de URL que tenha um site com vários domínios de nível superior (TLDs), cada TLS deve ser adicionado separadamente. Se adicionar um domínio ao grupo, todo o conteúdo localizado neste domínio e em todos os subdomínios (por exemplo, *sub.paginaexemplo.com*) será bloqueado ou permitido de acordo com sua escolha de ação baseada na URL.

Direitos de acesso

- **Permitir** - O acesso ao endereço URL/categoria será concedido.
- **Alertar** - Alerta o usuário sobre o endereço URL/categoria.
- **Bloquear** - Bloqueia o endereço URL/categoria.

URL ou **Usar grupo de URL** - Usa o link ou grupo de links de URL para permitir, bloquear ou alertar o usuário quando uma dessas URL for detectada.

Gravidade do registro em log:

- **Sempre** - Registra todas as comunicações on-line.
- **Diagnóstico** - Registra informações necessárias para ajustar o programa.
- **Informações** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Aviso** - Registra mensagens de erros críticos e de aviso.
- **Nenhum** - Nenhum relatório será criado.

Lista de usuários

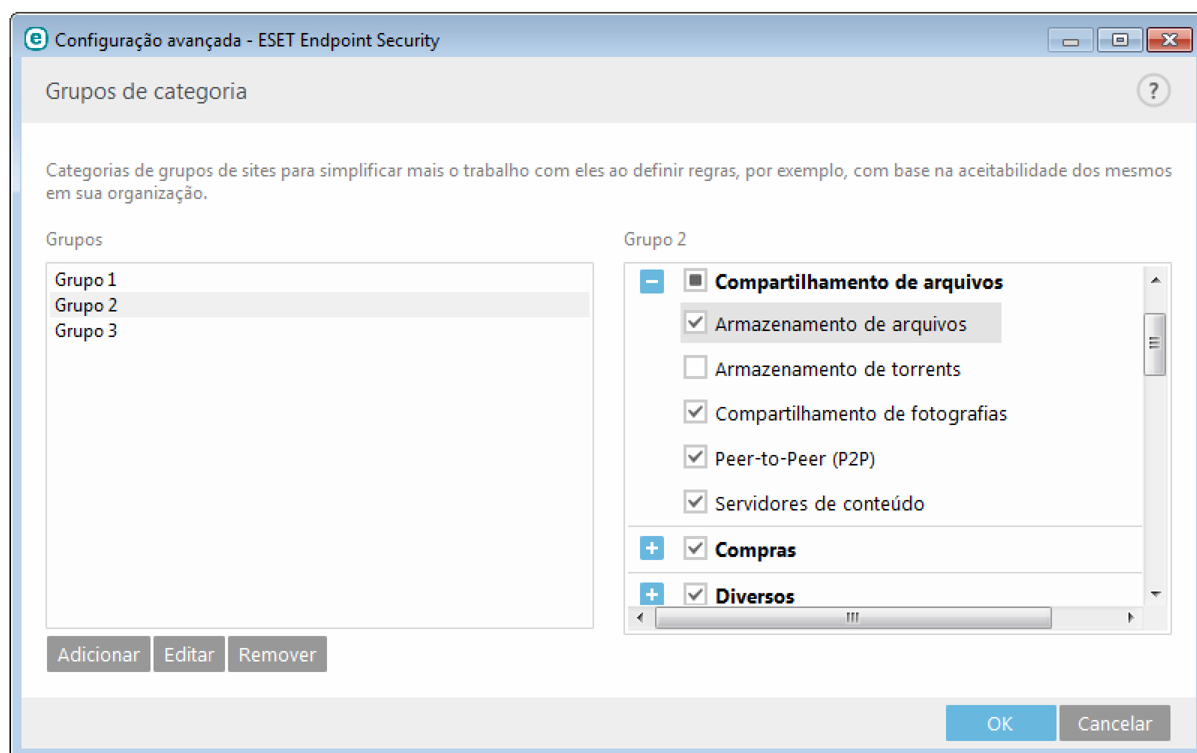
- **Adicionar** - Abra a janela de diálogo **Selecionar usuários ou grupos**, que permite que você selecione usuários desejados. Quando nenhum usuário for inserido, a regra será aplicada para todos os usuários.
- **Remover** - Remove o usuário selecionado do filtro.

3.8.4.2 Grupos de categoria

A janela Grupo de categoria é dividida em duas partes. A parte direita da janela contém uma lista de categorias e subcategorias. Selecione a categoria na lista Categoria para exibir suas subcategorias.

Cada grupo contém subcategorias geralmente inadequadas e/ou para adultos, bem como categorias consideradas geralmente aceitáveis. Quando você abrir a janela Grupos de categoria e clicar no primeiro grupo, poderá adicionar ou remover categorias/subcategorias da lista de grupos apropriados (por exemplo, violência ou armas). Páginas da Web com conteúdo inadequado podem ser bloqueadas ou usuários podem ser informados depois que uma regra com ações predefinidas for criada.

Marque a caixa de seleção para adicionar ou remover uma subcategoria para um grupo específico.



Aqui estão alguns exemplos de categorias com as quais os usuários podem não estar familiarizados:

Diversos - Geralmente, endereços IP privados (locais), como intranet, 192.168.0.0/16, etc. Quando você recebe um código de erro 403 ou 404, o site também corresponderá a essa categoria.
Não solucionado - Esta categoria inclui páginas da web não solucionadas devido a um erro ao se conectar ao mecanismo do banco de dados do Controle de Web.
Não categorizado - Páginas da Web desconhecidas que ainda não estão no banco de dados de controle da Web.
Proxies - Páginas da Web, como anonimizadores, redirecionadores ou servidores proxy públicos, podem ser usadas para obter acesso (anônimo) a páginas da web que geralmente são proibidas pelo filtro do Controle de Web.
Compartilhamento de arquivos - Estas páginas da web contêm grandes quantidades de dados, como fotos, vídeos ou livros eletrônicos. Há um risco de que esses sites possam conter materiais potencialmente ofensivos ou de conteúdo adulto.

OBSERVAÇÃO: Uma subcategoria pode pertencer a qualquer grupo. Existem algumas subcategorias que não estão incluídas nos grupos predefinidos (por exemplo, Jogos). Para corresponderem a uma subcategoria desejada usando o filtro de Controle de web, adicione-a a um grupo desejado.

3.8.4.3 Grupos de URL

O grupo de URL permite que você crie um grupo com vários links URL para os quais você deseja criar uma regra (permitir/bloquear certos sites).

Para criar um novo grupo de URL clique em **Adicionar**. Selecione um grupo de URL e clique em **Adicionar** na parte inferior direita da janela para adicionar um novo endereço URL à lista ou clique em **Importar** para importar um arquivo com uma lista de endereços URL (separe os valores com uma quebra de linha, por exemplo, *.txt usando a codificação UTF-8). Se você quiser definir uma ação a ser realizada para um grupo de URL específico, abra o **Editor de regras do controle da Web**, selecione seu grupo de URL usando o menu suspenso, ajuste outros parâmetros e clique em **OK**.

OBSERVAÇÃO: Bloquear ou permitir uma página da Web específica pode ser mais seguro do que bloquear ou permitir uma categoria inteira de páginas da Web. Tenha cuidado ao alterar essas configurações e adicionar uma página da Web ou categoria à lista.

3.8.5 Atualização do programa

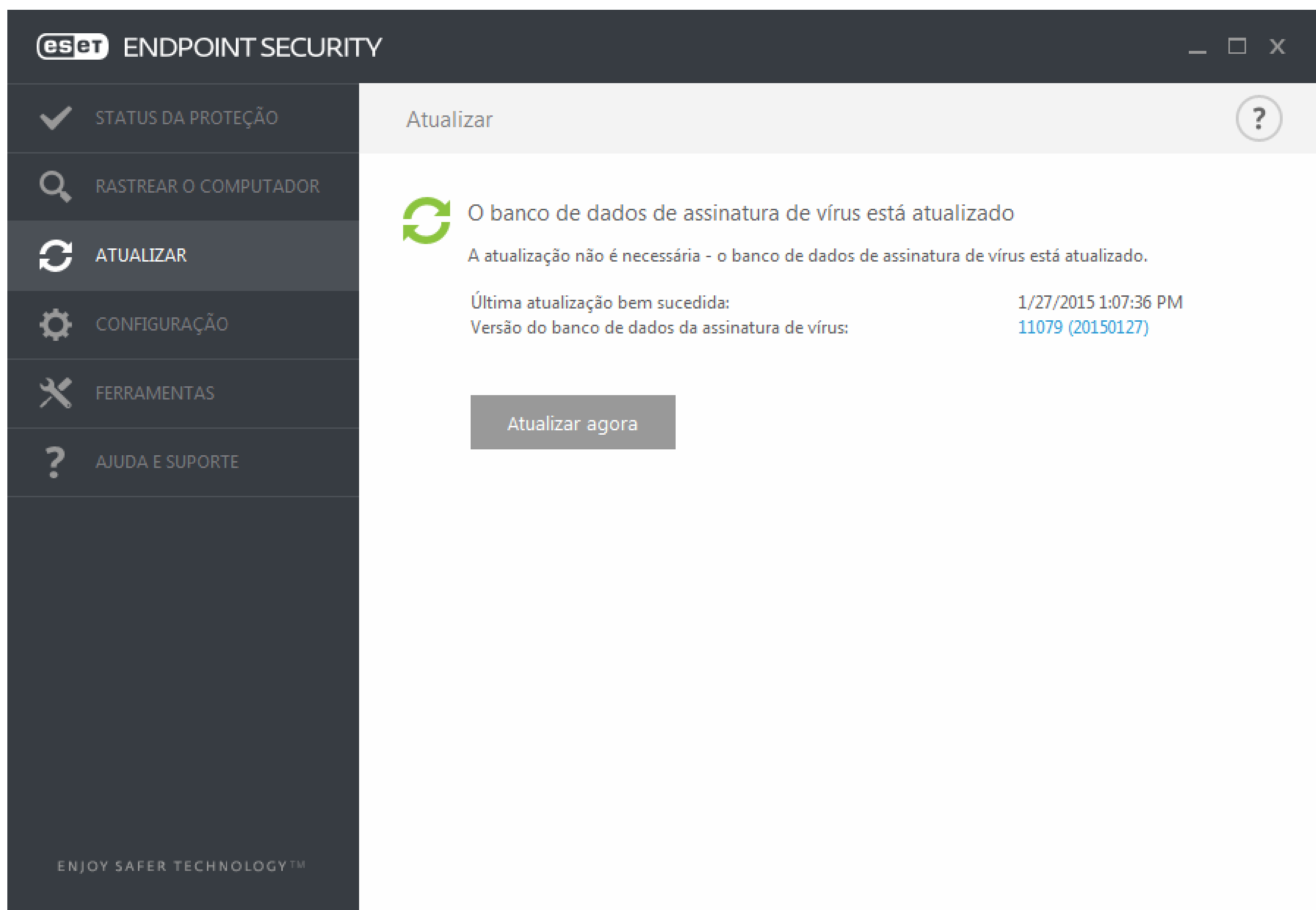
Atualizar o ESET Endpoint Security periodicamente é o melhor método para se obter o nível máximo de segurança em seu computador. O módulo de atualização garante que o programa está sempre atualizado de duas maneiras, atualizando o banco de dados de assinatura de vírus e atualizando os componentes do sistema.

Na janela principal do programa, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida e se uma atualização será necessária. A janela principal também contém a versão do banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas em determinada atualização.

Além disso, a opção para iniciar manualmente o processo de atualização **Atualizar banco de dados de assinatura de vírus**, está disponível. A atualização do banco de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes da manutenção da proteção completa contra códigos maliciosos. Dê atenção especial à sua configuração e operação. Se você não inseriu os detalhes da licença durante a instalação, você poderá inserir sua chave de licença clicando em **Ativar produto** ao atualizar para acessar os servidores de atualização da ESET.

Se você ativar o ESET Endpoint Security com o arquivo de licença off-line sem um Usuário e Senha e tentar atualizar, a informação em vermelho **A atualização do banco de dados de assinatura de vírus foi concluída com erro** sinaliza que você só poderá fazer download de atualizações da imagem.

OBSERVAÇÃO: Sua chave de licença é fornecida pela ESET após a compra do ESET Endpoint Security.

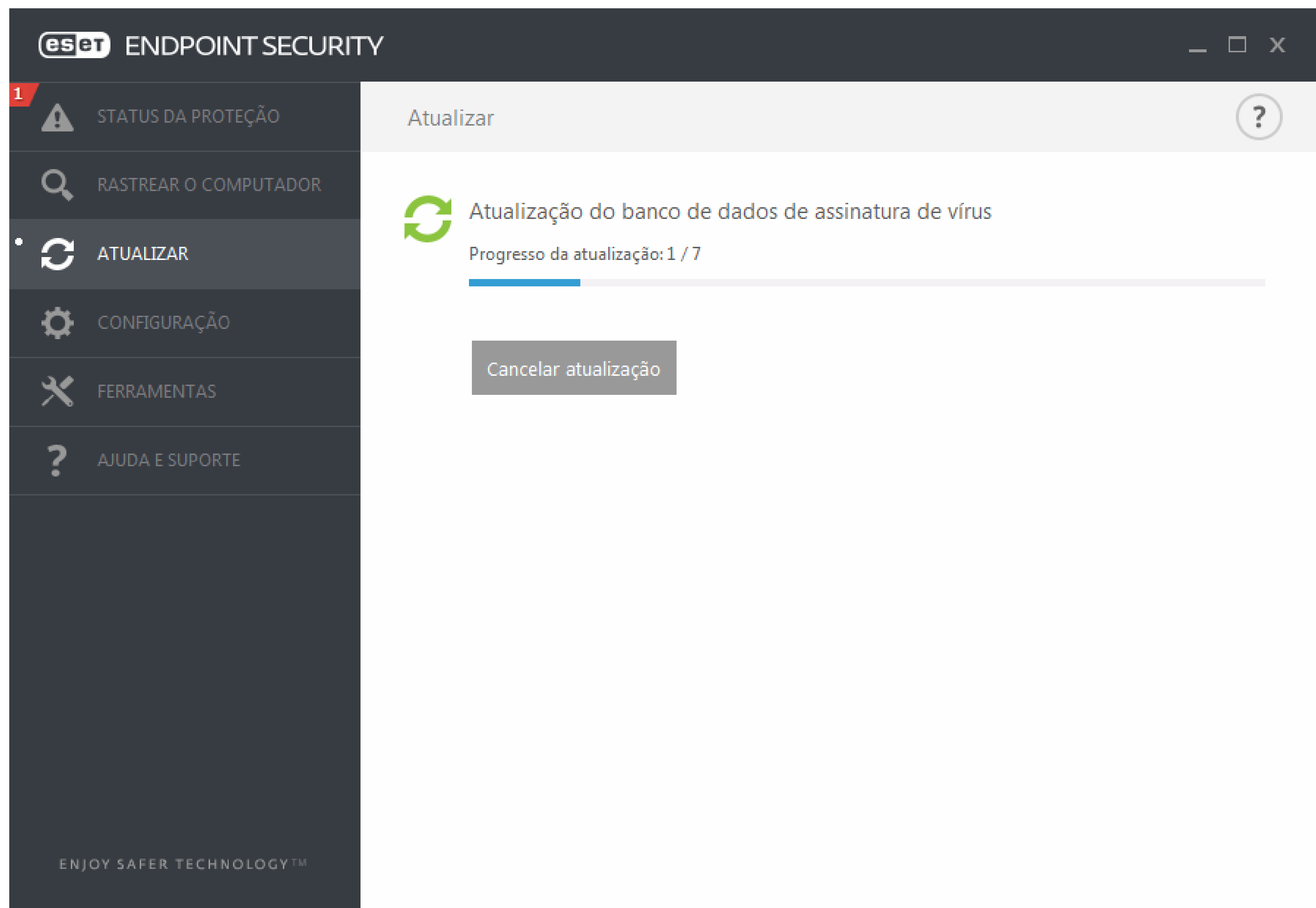


Última atualização bem-sucedida - A data da última atualização. Verifique se ela se refere a uma data recente, o que significa que o banco de dados de assinatura de vírus está atualizado.

Versão do banco de dados de assinatura de vírus – O número do banco de dados de assinatura de vírus, que também é um link ativo para o site da ESET. Clique para exibir uma lista de todas as assinaturas adicionadas na atualização.

Processo de atualização

Após clicar no botão **Atualizar banco de dados de assinatura de vírus**, o processo de download é iniciado. A barra de progresso do download e o tempo restante do download serão exibidos. Para interromper a atualização, clique em **Cancelar atualização**.

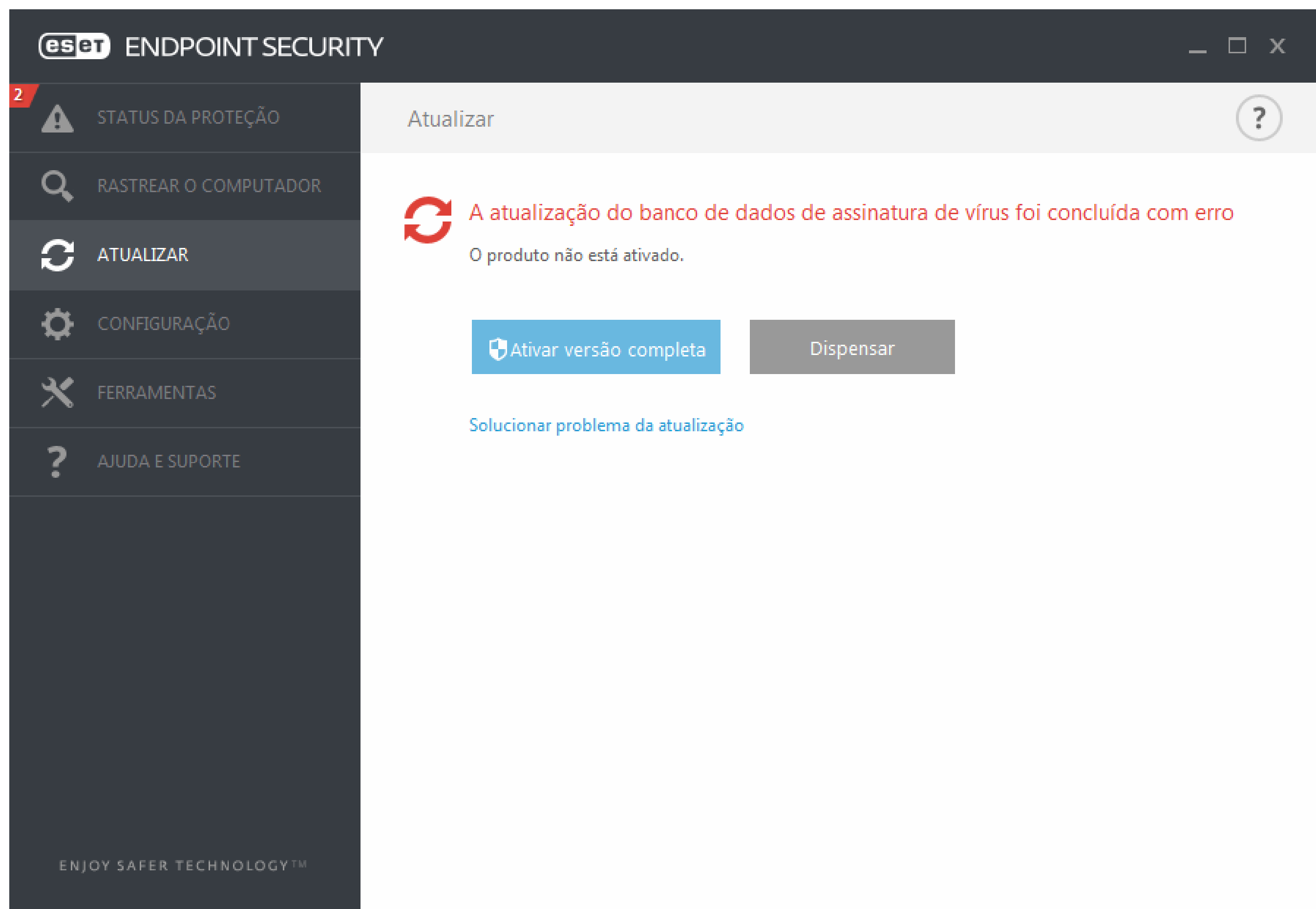


Importante: Em circunstâncias normais, quando o download das atualizações é feito adequadamente, a mensagem **A atualização não é necessária - O banco de dados de assinatura de vírus está atualizado** aparecerá na janela **Atualizar**. Se esse não for o caso, o programa estará desatualizado e mais vulnerável a uma infecção. Atualize o banco de dados de assinatura de vírus assim que for possível. Caso contrário, uma das seguintes mensagens será exibida:

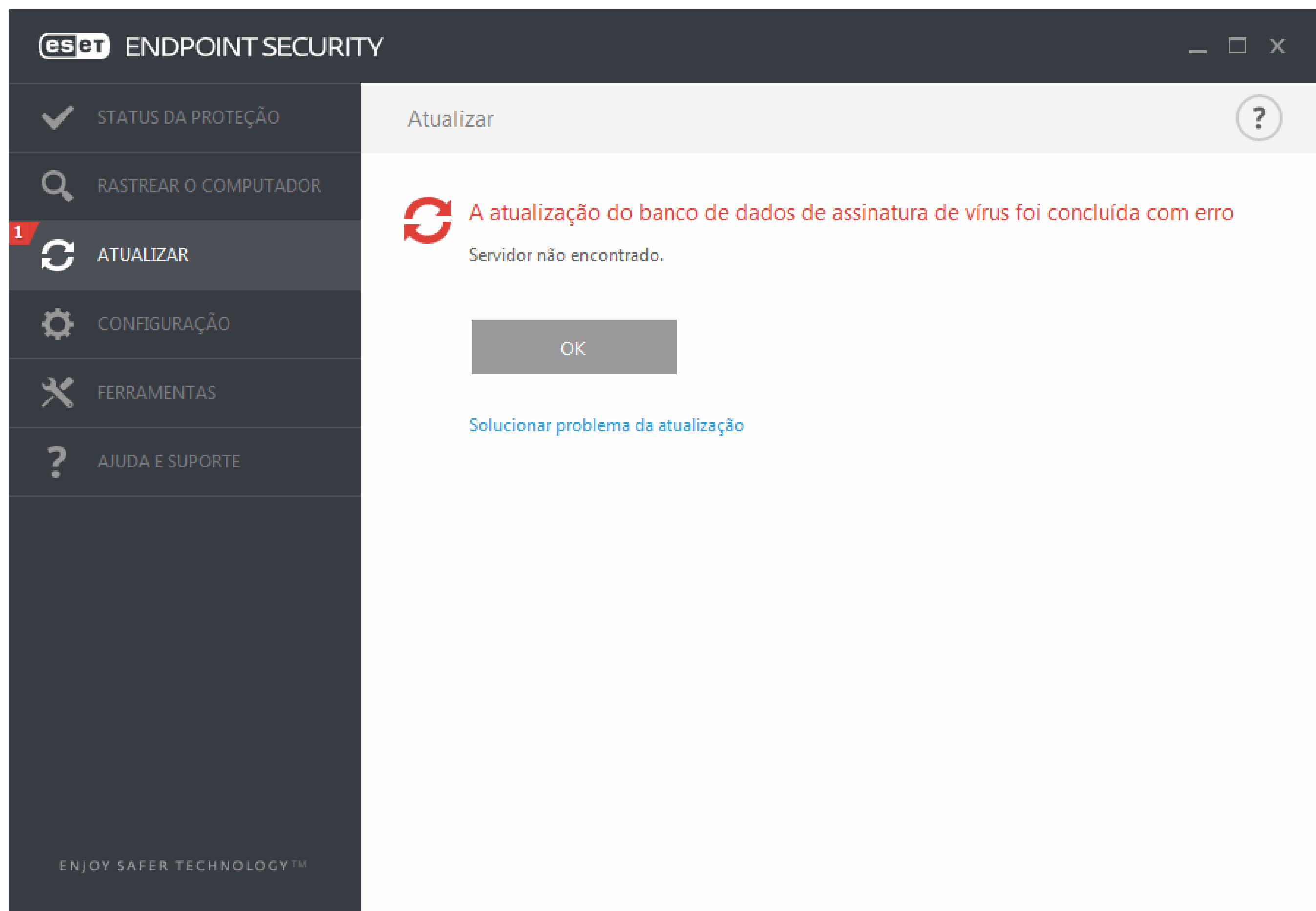
O banco de dados de assinatura de vírus está desatualizado - Esse erro aparecerá após diversas tentativas malsucedidas de atualizar o banco de dados de assinatura de vírus. Recomendamos que você verifique as configurações de atualização. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos ou definições incorretas das configurações de conexão.

A notificação anterior está relacionada às duas mensagens a seguir de **Falha na atualização do banco de dados de assinatura de vírus** sobre atualizações malsucedidas:

1. **Licença inválida** - A chave de licença foi inserida incorretamente na configuração da atualização. Recomendamos que você verifique os seus dados de autenticação. A janela Configuração avançada (no menu principal, clique em **Configuração** e depois em **Configuração avançada** ou pressione F5 no teclado) contém opções de atualização adicionais. Clique em **Ajuda e suporte** > **Gerenciar licenças** a partir do menu principal para inserir uma nova chave de licença.



2. **Ocorreu um erro durante o download dos arquivos de atualização** - Uma possível causa do erro pode dever-se a configurações de conexão à Internet incorretas. Recomendamos que você verifique a conectividade da Internet (abrindo qualquer site em seu navegador da Web). Se o site não abrir, é provável que uma conexão com a Internet não tenha sido estabelecida ou que haja problemas de conectividade com o seu computador. Verifique com o seu provedor de serviços de Internet (ISP) se você não tiver uma conexão ativa com a Internet.



OBSERVAÇÃO: Para obter mais informações, acesse este artigo da Base de conhecimento ESET.

3.8.5.1 Configuração da atualização

As opções de configuração da atualização estão disponíveis na árvore **Configuração avançada** (tecla F5) em **Atualizar** > **Básico**. Esta seção especifica as informações da origem da atualização, como, por exemplo, os servidores de atualização e os dados de autenticação sendo usados para esses servidores.

Geral

O perfil de atualização usado atualmente é exibido no menu suspenso **Perfil selecionado**. Para criar um novo perfil, clique em **Editar** ao lado de **Lista de perfis**, insira seu próprio **Nome de perfil** e então clique em **Adicionar**.

Se você está tendo dificuldade ao tentar fazer download das atualizações do banco de dados de assinatura de vírus, clique em **Limpar** para limpar os arquivos/cache de atualização temporários.

Alertas de banco de dados de assinatura de vírus desatualizado

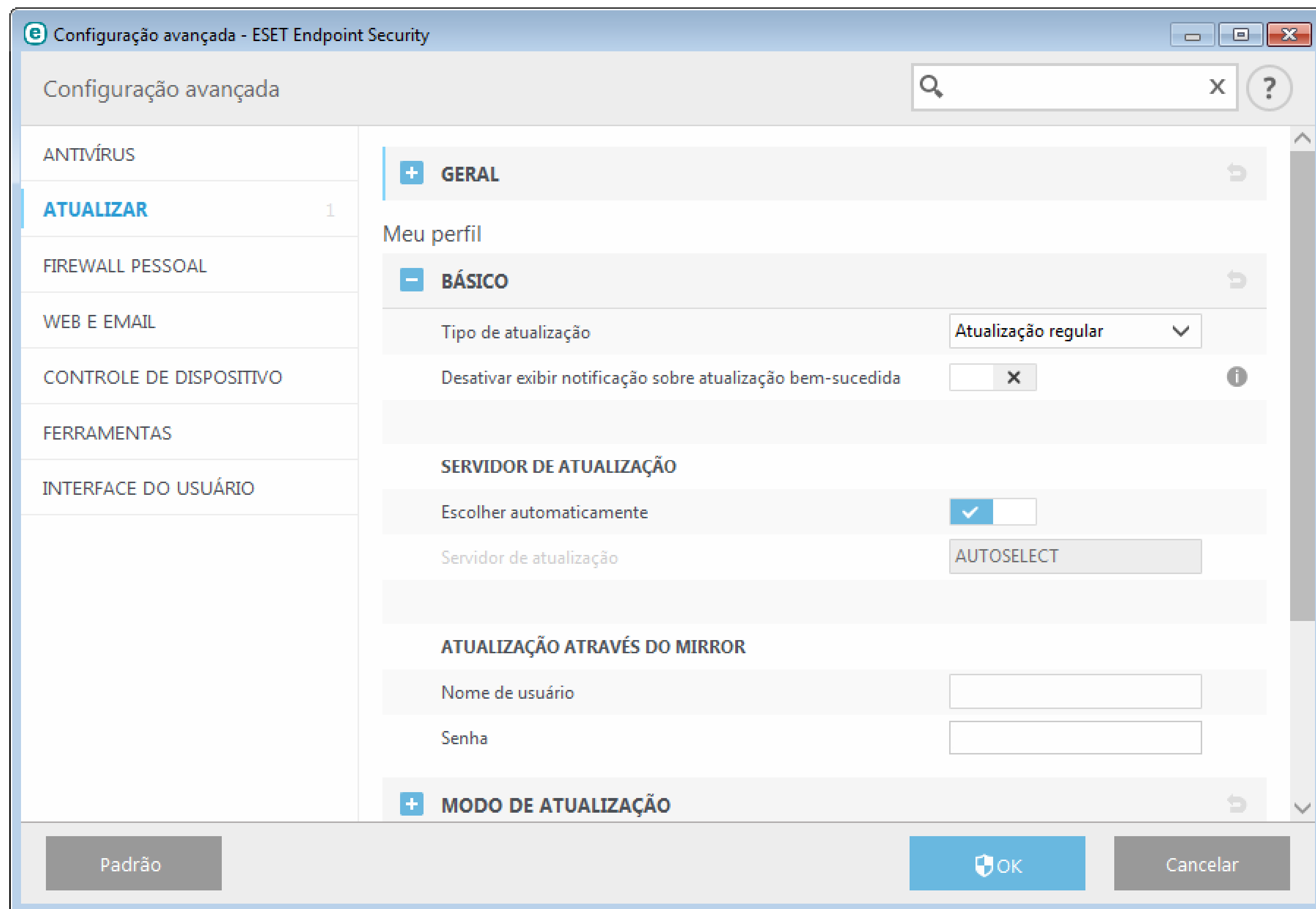
Definir a idade máxima do banco de dados automaticamente - Permite definir o tempo máximo (em dias) depois do qual o banco de dados de assinatura de vírus será relatado como desatualizado. O valor padrão é 7.

Rollback

Caso suspeite que uma nova atualização do banco de dados de vírus e/ou módulos do programa esteja instável ou corrompida, será possível reverter para a versão anterior e desativar atualizações por um período de tempo definido. Alternativamente, será possível ativar atualizações desativadas anteriormente caso tenha as adiado indefinidamente.

O ESET Endpoint Security registra instantâneos de módulos do programa e banco de dados de assinatura de vírus para uso com o recurso de *rollback*. Para criar instantâneos do banco de dados de vírus, deixe a caixa de seleção **Criar instantâneos dos arquivos de atualização** marcada. O campo **Número de instantâneos armazenados localmente** define o número de instantâneos do banco de dados de vírus anterior armazenado.

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Geral**), você terá que selecionar um intervalo de tempo no menu suspenso que represente o período de tempo que o banco de dados da assinatura de vírus e as atualizações do módulo do programa serão pausadas.



Para que o download das atualizações seja feito de forma adequada, é fundamental preencher corretamente todos os parâmetros de atualização. Se você usar um firewall, certifique-se de que o programa da ESET tem permissão para comunicar com a Internet (por exemplo, comunicação HTTP).

Básico

Por padrão, o **Tipo de atualização** é definido como **Atualização regular** para garantir que os arquivos de atualização são obtidos por download automaticamente do servidor da ESET com o menor tráfego de rede. Atualizações em modo de teste (a opção **Modo de teste**) são atualizações que passaram por testes internos e estarão disponíveis ao público geral em breve. Ao ativar as atualizações em modo de teste você pode se beneficiar do acesso aos métodos de detecção e correções mais recentes. No entanto, o modo de teste pode não ser sempre estável, e NÃO DEVE ser usado em servidores de produção e estações de trabalho em que é necessário ter a máxima disponibilidade e estabilidade. **Atualização atrasada** permite atualizar a partir de servidores especiais de atualização que fornecem novas versões do banco de dados de vírus com um atraso de, pelo menos, X horas (isto é, bancos de dados testados em um ambiente real e, por isso, considerados como estáveis).

Desativar exibir notificação sobre atualização bem-sucedida - Desativa a notificação da bandeja do sistema no canto inferior direito da tela. A seleção dessa opção será útil se um aplicativo ou jogo de tela inteira estiver em execução. Lembre-se de que o Modo de apresentação desativará todas as notificações.

Por padrão, o menu **Servidor de atualização** está definido como SELEÇÃO AUTOMÁTICA. O servidor de atualização é o local onde as atualizações são armazenadas. Se você usar um servidor da ESET, recomendamos que você deixe a opção padrão selecionada.

Ao usar um servidor HTTP local - também conhecido como Mirror - o servidor de atualização deve ser definido da seguinte forma:
http://nome_computador_ou_seu_endereço_IP:2221

Ao usar um servidor HTTP local com SSL - o servidor de atualização deve ser definido da seguinte forma:
https://nome_computador_ou_seu_endereço_IP:2221

Ao usar uma pasta compartilhada local - o servidor de atualização deve ser definido da seguinte forma:
\\computer_name_or_its_IP_address\shared_folder

Atualização através da Imagem

A autenticação dos servidores de atualização é baseada no **Chave de licença** gerada e enviada ao usuário após a compra. Ao usar um servidor de imagem local, você pode definir credenciais para clientes para conexão no servidor de imagem antes do recebimento de atualizações. Por padrão, não é necessário verificação e os campos **Usuário** e **Senha** são deixados em branco.

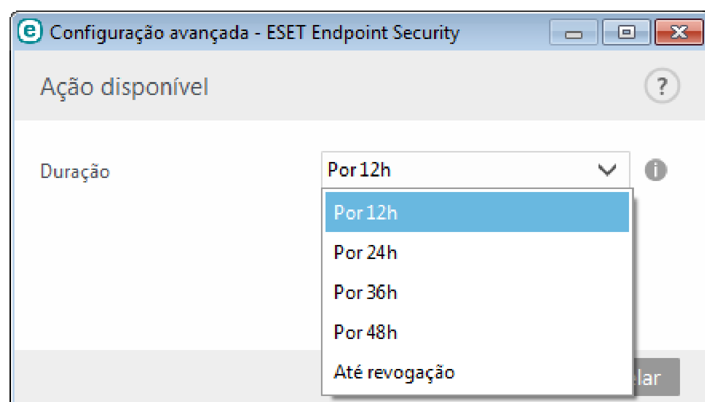
3.8.5.1.1 Atualizar perfis

Os perfis de atualização podem ser criados para várias configurações e tarefas de atualização. A criação de perfis de atualização é especialmente útil para usuários móveis, que precisam de um perfil alternativo para propriedades de conexão à Internet que mudam regularmente.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento, definido em **Meu perfil** por padrão. Para criar um novo perfil, clique em **Editar** ao lado de **Lista de perfis**, insira seu próprio **Nome de perfil** e então clique em **Adicionar**.

3.8.5.1.2 Rollback de atualização

Se você clicar em **Reverter** (**Configuração avançada** (F5) > **Atualizar** > **Perfil**), você terá que selecionar um intervalo de tempo no menu suspenso que represente o período de tempo que o banco de dados da assinatura de vírus e as atualizações do módulo do programa serão pausadas.



Selecione **Até cancelado** para adiar atualizações regulares indefinidamente até restaurar a funcionalidade de atualização manualmente. Pois isso representa um risco de segurança em potencial, não recomendamos a seleção desta opção.

A versão do banco de dados de assinatura de vírus é desatualizada para a versão mais antiga disponível e armazenada como um instantâneo no sistema de arquivos do computador local.

Exemplo: Permita que o número 10646 seja a versão mais atual do banco de dados de assinatura de vírus. 10645 e 10643 são armazenados como instantâneos do banco de dados de assinatura de vírus. Observe que 10644 não está disponível porque, por exemplo, o computador foi desligado e uma atualização mais recente foi disponibilizada antes de a 10644 ser baixada. Se você inseriu 2 (dois) no campo **Número de instantâneos armazenados localmente** e clicou em **Reverter**, o banco de dados de assinatura de vírus (incluindo módulos do programa) será restaurado para a versão número 10643. Este processo pode demorar algum tempo. Verifique se a versão do banco de dados de assinatura de vírus foi desatualizada na janela principal do programa do ESET Endpoint Security na seção Atualizar.

3.8.5.1.3 Modo de atualização

A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa. O programa permite que você pré-defina seu comportamento quando uma nova atualização de componentes está disponível.

As atualizações de componentes do programa oferecem novos recursos ou fazem alterações nos recursos já existentes de versões anteriores. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois de a atualização de componentes do programa ser instalada, pode ser necessário reiniciar seu computador. Na seção **Atualização de componente de programa**, três opções estão disponíveis:

- **Perguntar antes de fazer download dos componentes do programa** - Opção padrão. Você será solicitado a confirmar ou recusar as atualizações de componentes do programa quando elas estiverem disponíveis.
- **Sempre atualizar componentes do programa** - As atualizações de componentes do programa serão obtidas por download e instaladas automaticamente. Lembre-se de que pode ser necessário reiniciar o computador.
- **Nunca atualizar componentes do programa** - As atualizações de componentes do programa não serão realizadas. Esta opção é adequada para instalações de servidor, pois os servidores podem geralmente ser reiniciados somente quando estiverem em manutenção.

OBSERVAÇÃO: A seleção da opção mais apropriada depende da estação de trabalho em que as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar danos sérios.

Se a opção **Perguntar antes de fazer download da atualização** estiver ativa, uma notificação será exibida quando uma nova atualização estiver disponível.

Se o tamanho do arquivo de atualização for maior que o valor especificado no campo **Perguntar se um arquivo de atualização for maior que (KB)**, o programa exibirá uma notificação.

3.8.5.1.4 Proxy HTTP

Para acessar as opções de configuração do servidor proxy de determinado perfil de atualização, clique em **Atualizar** na árvore **Configuração avançada** (F5) e clique em **Proxy HTTP**. Clique no menu suspenso **Modo proxy** e selecione uma das três opções a seguir:

- Não usar servidor proxy
- Conexão através de um servidor proxy
- Usar configurações globais de servidor proxy

Selecione a opção **Usar configurações globais de servidor proxy** para usar as opções de configuração do servidor proxy já especificadas na ramificação **Ferramentas** > **Servidor proxy** da árvore Configuração avançada.

Selecione **Não usar servidor proxy** para especificar que nenhum servidor proxy será usado para atualizar o ESET Endpoint Security.

A opção **Conexão através de um servidor proxy** deve ser selecionada se:

- Deve ser usado um servidor proxy para atualizar o ESET Endpoint Security que seja diferente do servidor proxy especificado nas configurações globais (**Ferramentas** > **Servidor proxy**). Nesse caso, as configurações devem ser especificadas aqui: O endereço do **Servidor proxy**, a **Porta** de comunicação (por padrão, 3128), além do **Usuário** e **Senha** para o servidor proxy, se necessário.
- As configurações do servidor proxy não foram definidas globalmente, mas o ESET Endpoint Security irá estabelecer conexão com um servidor proxy para atualizações.
- Seu computador estabelece conexão com a Internet por meio de um servidor proxy. As configurações são obtidas do Internet Explorer durante a instalação do programa; no entanto, se forem alteradas posteriormente (por exemplo, se você alterar o seu provedor de Internet), verifique se as configurações do proxy HTTP estão corretas nesta janela. Caso contrário, o programa não conseguirá estabelecer uma conexão com os servidores de atualização.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

OBSERVAÇÃO: Os dados de autenticação, tais como **Usuário** e **Senha**, são destinados para acessar o servidor proxy.

Preencha esses campos somente se um nome de usuário e uma senha forem necessários. Observe que esses campos não são para seu nome de usuário/senha do ESET Endpoint Security e devem ser fornecidos somente se você souber que precisa de senha para acessar a Internet por meio de um servidor proxy.

3.8.5.1.5 Conectar na rede como

Ao atualizar a partir de um servidor local com uma versão do sistema operacional Windows NT, a autenticação para cada conexão de rede é necessária por padrão.

Para configurar uma conta deste tipo, selecione a partir do menu suspenso **Tipo de usuário local**:

- **Conta do sistema (padrão)**,
- **Usuário atual**,
- **Usuário especificado**.

Selecione a opção **Conta do sistema (padrão)** para utilizar a conta do sistema para autenticação. De maneira geral, nenhum processo de autenticação ocorre normalmente se não houver dados de autenticação na seção principal de configuração de atualização.

Para assegurar que o programa é autenticado usando uma conta de usuário conectado no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se ao servidor de atualização se nenhum usuário tiver feito logon no momento.

Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação. Use esse método quando a conexão com a conta do sistema padrão falhar. Lembre-se de que a conta do usuário especificado deve ter acesso ao diretório de arquivos de atualização no servidor local. Caso contrário, o programa não poderá estabelecer conexão e fazer download das atualizações.

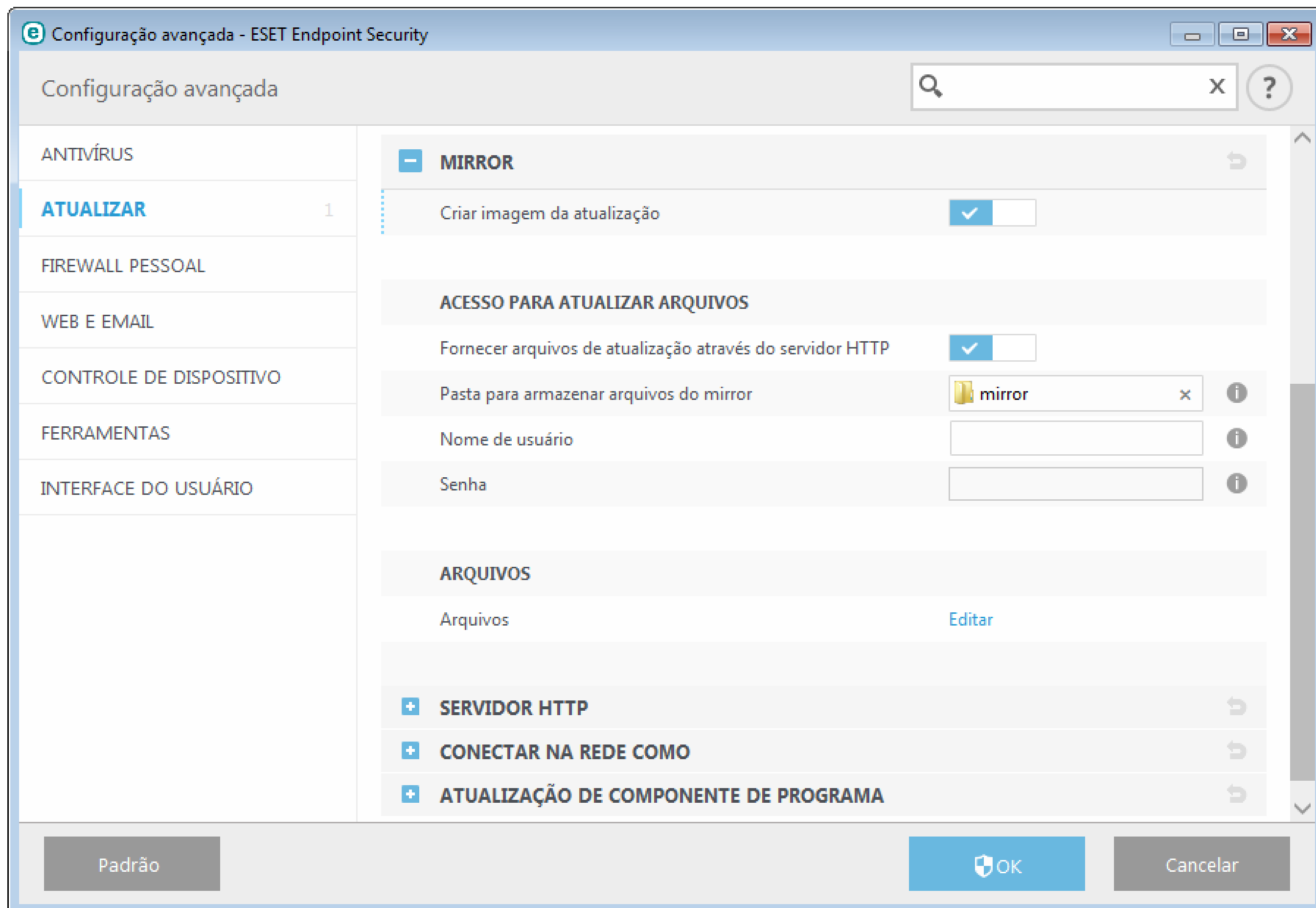
Aviso: Quando a opção **Usuário atual** ou **Usuário especificado** estiver selecionada, um erro poderá ocorrer ao alterar a identidade do programa para o usuário desejado. Recomendamos inserir os dados de autenticação da rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: *nome_domínio\usuário* (se for um grupo de trabalho, insira o *nome_do_grupo_de_trabalho\nome*) e a senha. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

Selecione **Desconectar do servidor depois da atualização** para forçar uma desconexão se a conexão com o servidor permanecer ativa mesmo depois de fazer o download das atualizações.

3.8.5.1.6 Mirror

O ESET Endpoint Security permite criar cópias dos arquivos de atualização, que podem ser usadas para atualizar outras estações de trabalho na rede. Uso de uma *"imagem"* - uma cópia dos arquivos de atualização no ambiente de rede local é conveniente, pois os arquivos de atualização não precisam ser obtidos por download a partir do servidor de atualização do fabricante repetidamente e por cada estação de trabalho. O download das atualizações é feito para o servidor de imagem local e, em seguida, distribuído a todas as estações de trabalho, evitando assim o risco de sobrecarga potencial do tráfego de rede. A atualização das estações clientes a partir de uma Mirror otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.

As opções de configuração do servidor local da Imagem estão localizadas em Configuração avançada em **Atualizar**. Para acessar esta seção pressione **F5** para acessar a Configuração avançada, clique em **Atualizar** e selecione a guia **Imagem**.



Para criar uma imagem na estação de trabalho do cliente, ative **Criar imagem da atualização**. Ativar essa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos serão acessados e o caminho de atualização para os arquivos da imagem.

Acesso para atualizar arquivos

Fornecer arquivos de atualização através do servidor HTTP interno - Se esta opção for ativada, os arquivos de atualização podem simplesmente ser acessados através de HTTP, sem a necessidade de credenciais.

OBSERVAÇÃO: O Windows XP precisa do Service Pack 2 ou posterior para usar o Servidor HTTP.

Os métodos de acesso do servidor de Imagem estão descritos em detalhes na seção Atualização através do Imagem. Há dois métodos básicos para acessar a Imagem - a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou os clientes podem acessar a imagem localizada em um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a Imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Clique em **Pasta** para procurar uma pasta no computador local ou em uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser fornecidos nos campos **Nome de usuário** e **Senha**. Se a pasta de destino selecionada estiver localizada em um disco de rede que esteja executando o sistema operacional Windows NT/2000/XP, o nome de usuário e a senha especificados devem ter privilégios de gravação para a pasta selecionada. O nome de usuário e a senha devem ser inseridos no formato *Domínio/Usuário* ou *Grupo de trabalho/Usuário*. Lembre-se de fornecer as senhas correspondentes.

Arquivos - Ao configurar a Imagem, é possível especificar as versões de idioma das atualizações que se deseja fazer download. Os idioma selecionados devem ser suportados pelo servidor de imagem configurado pelo usuário.

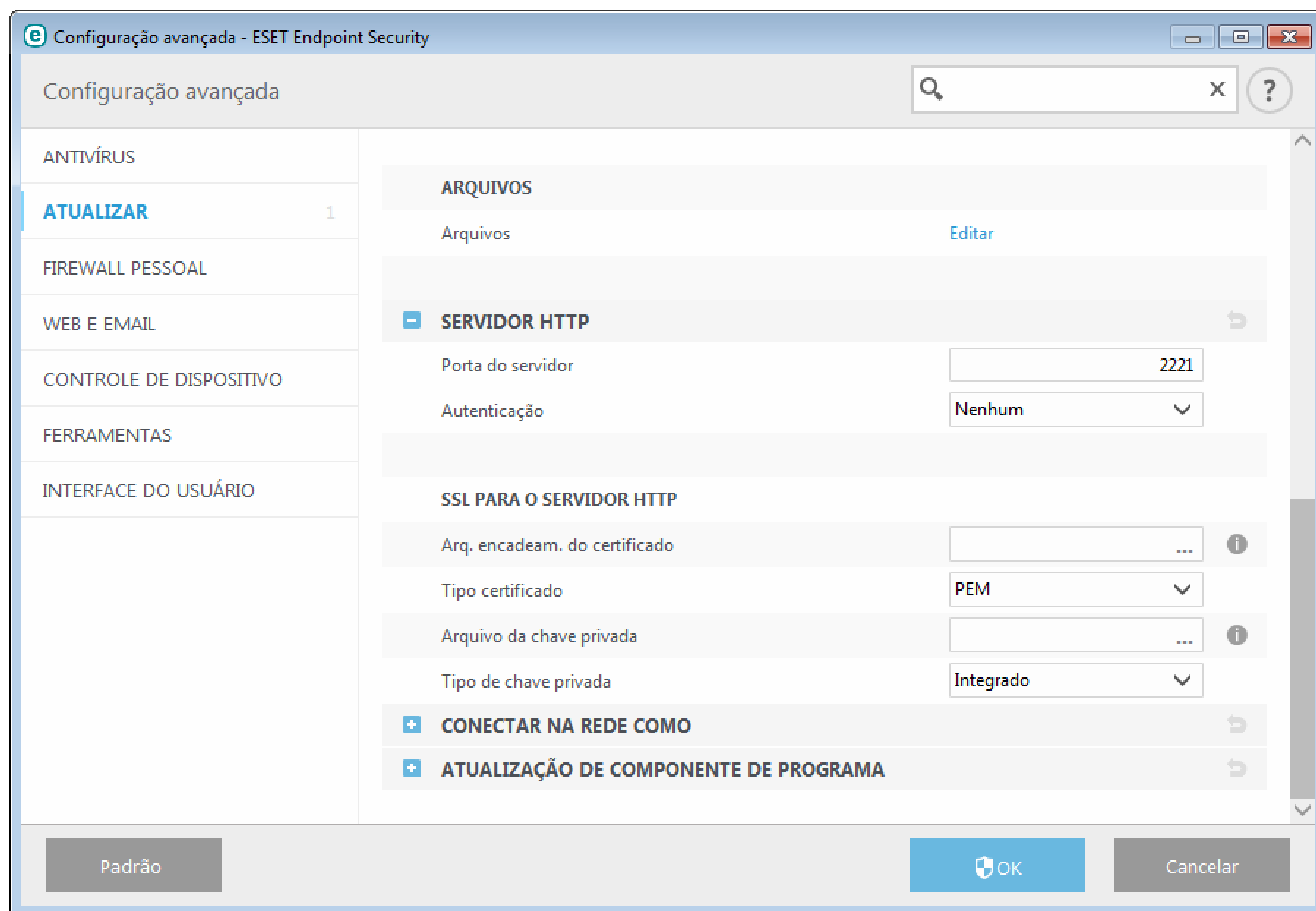
Servidor HTTP

Porta de servidor - Por padrão, a porta de servidor é definida como 2221.

Autenticação - Define o método de autenticação usado para acessar os arquivos de atualização. As opções disponíveis são: **Nenhum**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o

usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **Nenhum**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

Acrescente o **Arquivo de encadeamento do certificado** ou gere um certificado assinado automaticamente caso deseje executar o servidor HTTP com suporte HTTPS (SSL). Os seguintes tipos de certificado estão disponíveis: ASN, PEM e PFX. É possível fazer download dos arquivos de atualização através do protocolo HTTPS, que fornece mais segurança. É quase impossível rastrear transferências de dados e credenciais de login usando esse protocolo. A opção **Tipo de chave privada** é definida como **Integrada** por padrão, (portanto a opção de **Chave privada de arquivo** está desativada por padrão). Isso significa que a chave privada é uma parte do arquivo de encadeamento do certificado selecionado.



Conectar na rede como

Tipo de usuário local - As configurações **Conta do sistema (padrão)**, **Usuário atual** e **Usuário especificado** serão exibidas nos menus suspensos correspondentes. As configurações **Nome** e **Senha** são opcionais. Consulte Conectar na rede como.

Selecione **Desconectar do servidor depois da atualização** para forçar uma desconexão se a conexão com o servidor permanecer ativa depois de fazer o download das atualizações.

Atualização de componente de programa

Atualizar componentes automaticamente - Permite a instalação de novos recursos e atualizações para recursos existentes. Ela pode ser realizada automaticamente sem intervenção do usuário ou você pode escolher ser notificado. Depois de a atualização de componentes do programa ser instalada, pode ser necessário reiniciar seu computador.

Atualizar componentes agora - Atualiza seus componentes do programa para a versão mais recente.

3.8.5.1.6.1 Atualização através do mirror

Existem dois métodos básicos para configurar uma Imagem, que é essencialmente um repositório onde os clientes podem fazer download de arquivos de atualização. A pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou como um servidor HTTP.

Acesso à Mirror utilizando um servidor HTTP interno

Essa é a configuração padrão especificada na configuração do programa predefinida. Para permitir o acesso à Imagem utilizando o servidor HTTP, navegue até **Configuração avançada** > **Atualizar** > **Imagem** e selecione **Criar imagem da atualização**.

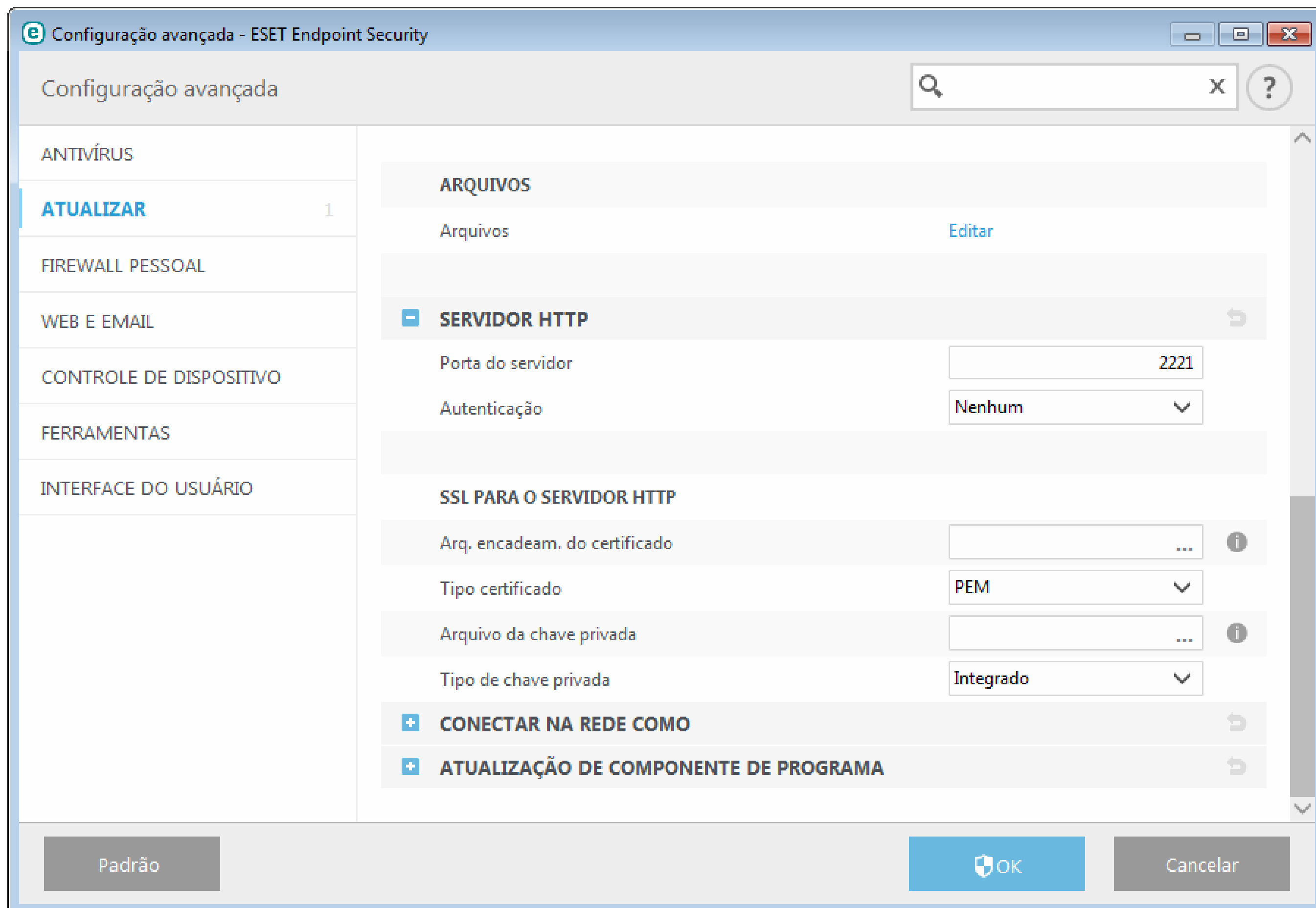
Na seção **Servidor HTTP** da guia **Mirror**, é possível especificar a **Porta do servidor**, em que o servidor HTTP escutará, bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a porta do servidor está definida em **2221**. A opção **Autenticação** define o método de autenticação usado para acessar os arquivos de atualização. As opções disponíveis são: **Nenhum**, **Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação através de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **Nenhum**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

Aviso: Se deseja permitir acesso aos arquivos de atualização através do servidor HTTP, a pasta Mirror deve estar localizada no mesmo computador que a instância do ESET Endpoint Security que os criou.

SSL para o servidor HTTP

Acrescente o **Arquivo de encadeamento do certificado** ou gere um certificado assinado automaticamente caso deseje executar o servidor HTTP com suporte HTTPS (SSL). Os seguintes tipos de certificado estão disponíveis: **PEM, PFX** e **ASN**. É possível fazer download dos arquivos de atualização através do protocolo HTTPS, que fornece mais segurança. É quase impossível rastrear transferências de dados e credenciais de login usando esse protocolo. A opção **Tipo chave privada** é definida como **Integrada** por padrão, o que significa que a chave privada é uma parte do arquivo de encadeamento do certificado selecionado.

OBSERVAÇÃO: Um erro **Nome de usuário e/ou senha inválidos** aparecerá no Painel de atualização a partir do menu principal após diversas tentativas mal sucedidas de atualizar o banco de dados de assinatura de vírus a partir da Imagem. Recomendamos ir para **Configuração avançada** > **Atualizar**> **Imagem** e verificar o Nome de usuário e a Senha. A razão mais comum para esse erro é a inserção de dados de autenticação incorretos.



Após concluir a configuração do servidor de Mirror, você deve adicionar o novo servidor de atualização em estações de trabalho clientes. Para fazer isso, siga as etapas a seguir:

- Acesse **Configuração avançada** (F5) e clique em **Atualizar** > **Básico**.
- Desative **Escolher automaticamente** e adicione um novo servidor ao campo **Servidor de atualização** usando um dos formatos a seguir:
  http://endereço_IP_do_seu_servidor:2221
  https://IP_address_of_your_server:2221 (se SSL for usado)

Acesso à Mirror por meio de compartilhamentos de sistema

Primeiro, uma pasta compartilhada deve ser criada em um dispositivo de rede ou local. Ao criar a pasta para a Mirror, é necessário fornecer acesso de *"gravação"* para o usuário que salvará os arquivos de atualização na pasta e acesso de *"leitura"* para todos os usuários que atualizarão o ESET Endpoint Security a partir da pasta Mirror.

Depois configure o acesso à Imagem na guia **Configuração avançada** > **Atualizar**> **Imagem** desativando a opção **Fornecer arquivos atualizados através do servidor HTTP interno**. Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador na rede, será necessário inserir os dados de autenticação para acessar o outro computador. Para inserir os dados de autenticação, abra a Configuração avançada do ESET Endpoint Security (F5) e clique em **Atualizar** > **Conectar na rede como**. Essa configuração é a mesma para a atualização, conforme descrito na seção Conectar na rede como.

Após concluir a configuração da Mirror, prossiga até as estações de trabalho e configure *\\UNC\PATH* como o servidor de atualização usando estas etapas:

1. Abra o ESET Endpoint Security **Configuração avançada** e clique em **Atualizar** > **Básico**.
2. Clique no campo **Servidor de atualização** e adicione um novo servidor usando o formato *\\UNC\PATH*.

OBSERVAÇÃO: Para o funcionamento correto das atualizações, o caminho para a pasta Mirror deve ser especificado como um caminho UNC. A atualização das unidades mapeadas pode não funcionar.

A última seção controla os componentes do programa (PCUs). Por padrão, os componentes de programas baixados são preparados para copiar para a imagem local. Se **Atualizar componentes do programa** estiver ativado, não é necessário clicar em **Atualizar** porque os arquivos são copiados para a imagem local automaticamente quando estiverem disponíveis. Consulte Modo de atualização para obter mais informações sobre as atualizações dos componentes do programa.

3.8.5.1.6.2 Solução de problemas de atualização através da imagem

Na maioria dos casos, os problemas que ocorrem durante a atualização do servidor de imagem são causados por um ou mais dos seguintes itens: especificação incorreta das opções da pasta Mirror, dados de autenticação incorretos para a pasta Mirror, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização a partir da Mirror ou por uma combinação das razões citadas. A seguir, é fornecida uma visão geral dos problemas mais frequentes que podem ocorrer durante uma atualização da Mirror:

O **ESET Endpoint Security relata um erro ao conectar a um servidor de imagem** - provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Mirror), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique no menu **Iniciar** do Windows, clique em **Executar**, insira o nome da pasta e clique em **OK**. O conteúdo da pasta deve ser exibido.

O **ESET Endpoint Security requer um nome de usuário e senha** - Provavelmente provocado por dados de autenticação incorretos (nome de usuário e senha) na seção de atualização. O nome do usuário e a senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa se atualizará. Verifique se os dados de autenticação estão corretos e inseridos no formato correto. Por exemplo, *Domínio/Nome de usuário* ou *Grupo de trabalho/Nome de usuário*, além das senhas correspondentes. Se o servidor de imagem puder ser acessado por "Todos", esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. "Todos" não significa qualquer usuário não autorizado, apenas significa que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta puder ser acessada por "Todos", um nome de usuário e uma senha do domínio ainda precisarão ser inseridos na seção de configuração da atualização.

O **ESET Endpoint Security relata um erro ao conectar a um servidor de imagem** - A comunicação na porta definida para acessar a versão HTTP da Mirror está bloqueada.

3.8.5.2 Como criar tarefas de atualização

As atualizações podem ser acionadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela principal, exibida depois de clicar em **Atualizar** no menu principal.

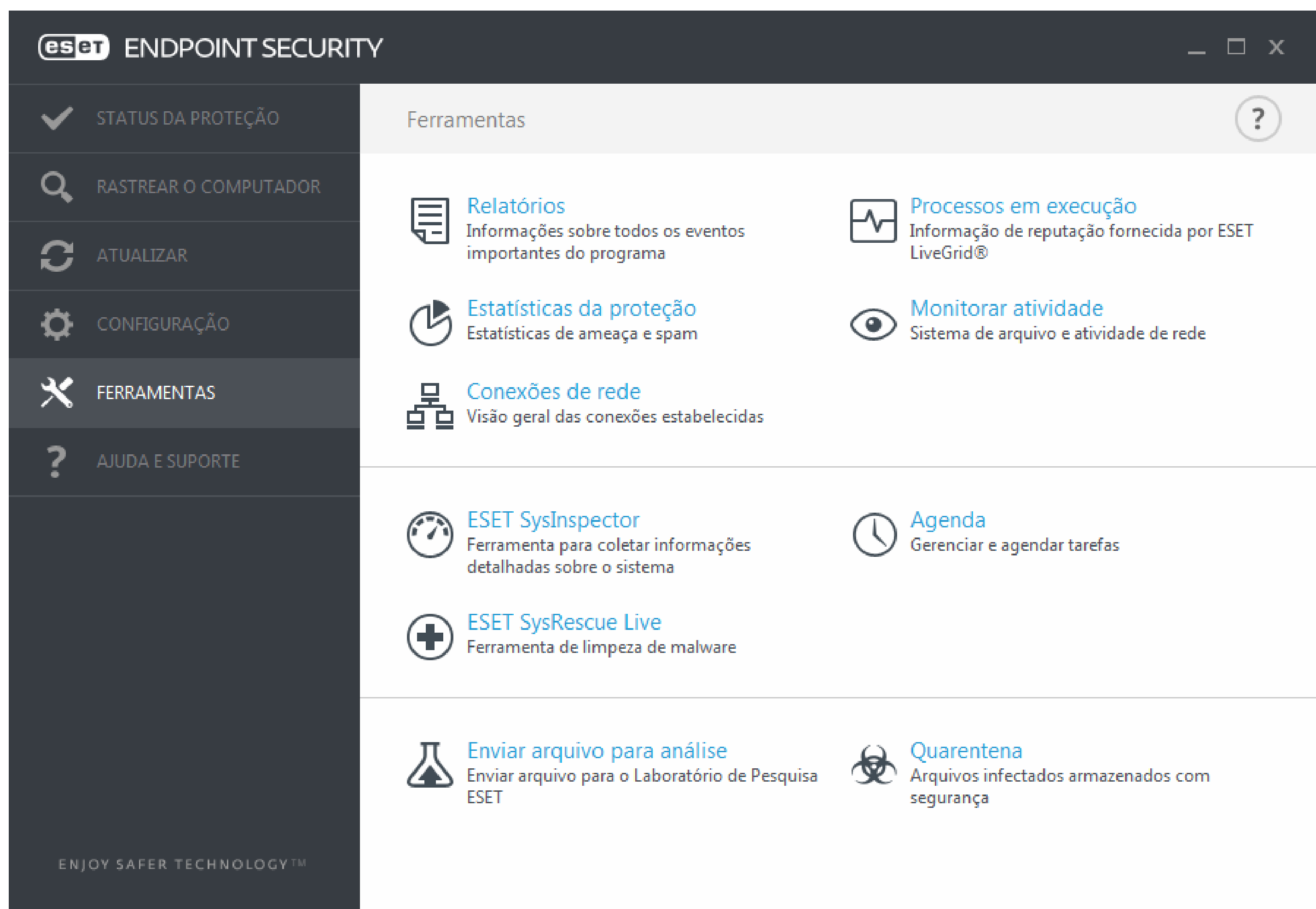
As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas estão ativadas no ESET Endpoint Security:

- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**

Toda tarefa de atualização pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte Agenda.

3.8.6 Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.



Esse menu inclui as seguintes ferramentas:

- Relatórios
- Estatísticas da proteção
- Monitorar atividade
- Processos em execução (se o ESET Live Grid estiver ativado no ESET Endpoint Security)
- Agenda
- Quarentena
- Conexões de rede (se o estiver ativado no ESET Endpoint Security)
- ESET SysInspector

Enviar amostra para análise - Permite enviar um arquivo suspeito aos Laboratórios de pesquisa da ESET para análise. A janela de diálogo exibida depois de clicar nessa opção é descrita na seção Envio de arquivos para análise.

ESET SysRescue - Redireciona você para a página do ESET SysRescue Live, onde é possível fazer download da imagem do ESET SysRescue Live ou Live CD/USB Creator para sistemas operacionais do Microsoft Windows.

3.8.6.1 Arquivos de log

Os arquivos de log contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em log atua como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em log realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do log. É possível visualizar mensagens de texto e logs diretamente do ambiente do ESET Endpoint Security, bem como arquivar relatórios.

Os arquivos de log podem ser acessados na janela principal do programa, clicando em **Ferramentas** > **Arquivos de log**. Selecione o tipo de log desejado no menu suspenso **Log**. Os seguintes logs estão disponíveis:

- **Ameaças detectadas** - O log de ameaças fornece informações detalhadas sobre as infiltrações detectadas pelos módulos do ESET Endpoint Security. As informações incluem a hora da detecção, nome da ameaça, local, ação realizada e o nome do usuário conectado no momento em que a ameaça foi detectada. Clique duas vezes em qualquer entrada de log para exibir seus detalhes em uma janela separada.
- **Eventos** - Todas as ações importantes executadas pelo ESET Endpoint Security são registradas no log de eventos. O log de eventos contém informações sobre eventos e erros que ocorreram no programa. Essa opção foi desenvolvida para ajudar administradores do sistema e usuários na solução de problemas. Muitas vezes as informações encontradas aqui podem ajudá-lo a encontrar uma solução para um problema no programa.
- **Rastrear o computador** - Todos os resultados de rastreamento são exibidos nesta janela. Cada linha corresponde a um rastreamento no computador. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo rastreamento.
- **HIPS** - Contém registros de regras específicas que foram marcadas para registro. O protocolo exibe o aplicativo que acionou a operação, o resultado (se a regra foi permitida ou proibida) e o nome da regra criada.
- **Firewall pessoal** - O log do firewall exibe todos os ataques remotos detectados pelo firewall pessoal. Aqui, você vai encontrar informações sobre todos os ataques em seu computador. A coluna *Evento* lista os ataques detectados. A coluna *Origem* informa mais sobre quem atacou. A coluna *Protocolo* revela o protocolo de comunicação usado para o ataque. A análise do log do firewall pode ajudá-lo a detectar tentativas de infiltração do sistema a tempo de evitar o acesso sem autorização ao sistema. Para obter mais detalhes sobre ataques de rede específicos, consulte Opções avançadas e IDS.
- **Sites filtrados** - Esta lista é útil se você quiser visualizar uma lista de sites que foram bloqueados pela Proteção de acesso à Web ou Controle de Web. Nesses logs, você poderá ver o horário, URL, usuário e aplicativo que criaram uma conexão para o site específico.
- **Proteção antispam** - Contém registros relacionados com emails marcados como spam.
- **Controle de Web** - Mostra endereços URL bloqueados ou permitidos e detalhes sobre suas categorias. A coluna *Ação executada* mostra como as regras de filtragem foram aplicadas.
- **Controle de dispositivos** - Contém registros de dispositivos ou mídias removíveis que foram conectados ao computador. Apenas dispositivos com regra de controle de dispositivo respectiva serão registrados no relatório. Se a regra não coincidir com um dispositivo conectado, uma entrada de log para um dispositivo conectado não será criada. Aqui, você também pode visualizar detalhes, como tipo de dispositivo, número de série, nome do fornecedor e tamanho da mídia (se disponível).

Em cada seção, as informações exibidas podem ser copiadas para a área de transferência (atalho do teclado: **Ctrl + C**), selecionando a entrada e clicando em **Copiar**. Para selecionar várias entradas, as teclas **Ctrl** e **Shift** podem ser usadas.

Clique em **Filtragem** para abrir a janela **Filtragem de relatórios** onde poderá definir os critérios de filtragem.

Você pode exibir o menu de contexto clicando com o botão direito em um registro específico. As seguintes opções também estão disponíveis no menu de contexto.

- **Mostrar** - Mostra informações mais detalhadas sobre o log selecionado em uma nova janela.
- **Filtrar registros do mesmo tipo** - Depois de ativar esse filtro, você só verá registros do mesmo tipo (diagnósticos, avisos...).
- **Filtrar.../Localizar...** - Depois de clicar nessa opção, a janela Pesquisar no log permitirá que você defina critérios de filtragem para entradas de log específicas.
- **Ativar filtro** - Ativa configurações de filtro.
- **Desativar filtro** - Apaga todas as configurações do filtro (conforme descrição acima).
- **Copiar/Copiar tudo** - Copia informações sobre todos os registros na janela.
- **Excluir/Excluir tudo** - Exclui o(s) registro(s) selecionado(s) ou todos os exibidos - essa ação requer privilégios de administrador.
- **Exportar...** - Exporta informações sobre o(s) registro(s) em formato XML.
- **Exportar todos...** - Exporta informações sobre todos os registros em formato XML.
- **Relatório de rolagem** - Deixe esta opção ativada para percorrer automaticamente logs antigos e monitorar logs ativos na janela **Relatórios**.

3.8.6.1.1 Pesquisar no log

Registra em log as informações de armazenamento sobre eventos importantes do sistema: O recurso de filtragem de logs permite exibir registros sobre um tipo específico de evento.

Insira a palavra-chave no campo **Localizar texto**. Se desejar pesquisar a palavra-chave em colunas específicas, altere o filtro no menu suspenso **Pesquisar nas colunas**.

Tipos de registro - Escolha um ou mais tipos de log de registro no menu suspenso:

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus, firewall integrado, etc...).

Período de tempo - Defina o período de tempo no qual deseja que os resultados sejam exibidos.

Coincidir apenas palavras inteiras - Marque essa caixa de seleção se você quiser pesquisar por palavras específicas para obter resultados mais precisos.

Diferenciar maiúsculas de minúsculas - Ative essa opção se for importante para você usar letras maiúsculas e minúsculas na filtragem.

Pesquisar no início - Resultados de pesquisa que aparecem no início do documento serão exibidos primeiro.

3.8.6.2 Configuração do servidor proxy

Em grandes redes LAN, a comunicação entre seu computador e a Internet pode ser mediada por um servidor proxy. Usando esta configuração, as configurações a seguir precisarão ser definidas. Caso contrário, o programa não poderá se atualizar automaticamente. No ESET Endpoint Security, a configuração do servidor proxy está disponível a partir de duas seções diferentes na árvore Configuração avançada.

As configurações do servidor proxy podem ser definidas em **Configuração avançada**, em **Ferramentas** > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Endpoint Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, selecione **Usar servidor proxy** e digite o endereço do servidor proxy no campo **Servidor proxy**, junto com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy exigir autenticação, selecione **O servidor proxy requer autenticação** e digite

um **Nome de usuário** e uma **Senha** válidos nos respectivos campos. Clique em **Detectar** para detectar e preencher automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados.

OBSERVAÇÃO: É preciso inserir manualmente seu Nome de usuário e Senha nas configurações do **Servidor proxy**.

Configurações do servidor proxy também podem ser estabelecidas na Configuração avançada de atualização (**Configuração avançada**> **Atualizar** > **Proxy HTTP** ao selecionar **Conexão através de um servidor proxy** no menu suspenso **Modo proxy**). Essa configuração será aplicada ao perfil de atualização especificado e é recomendada para laptops que recebem frequentemente atualizações de assinatura de vírus de locais remotos. Para obter mais informações sobre essa configuração, consulte Configuração avançada de atualização.

3.8.6.3 Agenda

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas.

A Agenda pode ser acessada na janela principal do programa do ESET Endpoint Security em **Ferramentas** > **Agenda**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.

O Agendador serve para agendar as seguintes tarefas: atualização do banco de dados das assinaturas de vírus, tarefa de rastreamento, rastreamento de arquivos na inicialização do sistema e manutenção do log. Você pode adicionar ou excluir tarefas diretamente da janela principal da Agenda (clique em **Adicionar tarefa** ou **Excluir** na parte inferior). Clique com o botão direito em qualquer parte na janela de Agenda para realizar as seguintes ações: exibir informações detalhadas, executar a tarefa imediatamente, adicionar uma nova tarefa e excluir uma tarefa existente. Use as caixas de seleção no início de cada entrada para ativar/desativar as tarefas.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Manutenção de logs**
- **Atualização automática de rotina**
- **Atualização automática após conexão dial-up**
- **Atualização automática após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após logon do usuário)
- **Rastreamento de arquivos em execução durante inicialização do sistema** (após atualização bem sucedida do banco de dados de assinatura de vírus)
- **Primeiro rastreamento automático**

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificar e clique no botão **Editar**.

Adicionar uma nova tarefa

1. Clique em **Adicionar tarefa** na parte inferior da janela.

2. Insira um nome da tarefa.

3. Selecione a tarefa desejada no menu suspenso:

- **Executar aplicativo externo** - Agenda a execução de um aplicativo externo.
- **Manutenção de logs** - Os relatórios também contêm registros remanescentes excluídos. Essa tarefa otimiza regularmente os registros nos relatórios para funcionar de maneira eficiente.
- **Verificar arquivos na inicialização do sistema** - Verifica os arquivos que estão permitidos para serem executados no logon ou na inicialização do sistema.
- **Criar um rastreamento do computador** - Cria um instantâneo do computador ESET SysInspector - coleta informações detalhadas sobre os componentes do sistema (por exemplo, drivers e aplicativos) e avalia o nível de risco de cada componente.
- **Rastrear o computador sob demanda** - Executa um rastreamento de arquivos e pastas em seu computador.
- **Primeiro rastreamento** - Por padrão, 20 minutos depois da instalação ou reinicialização um rastreamento do computador será executado como uma tarefa de baixa prioridade.
- **Atualização** - Agenda uma tarefa de atualização, atualizando o banco de dados de assinatura de vírus e os módulos do programa.

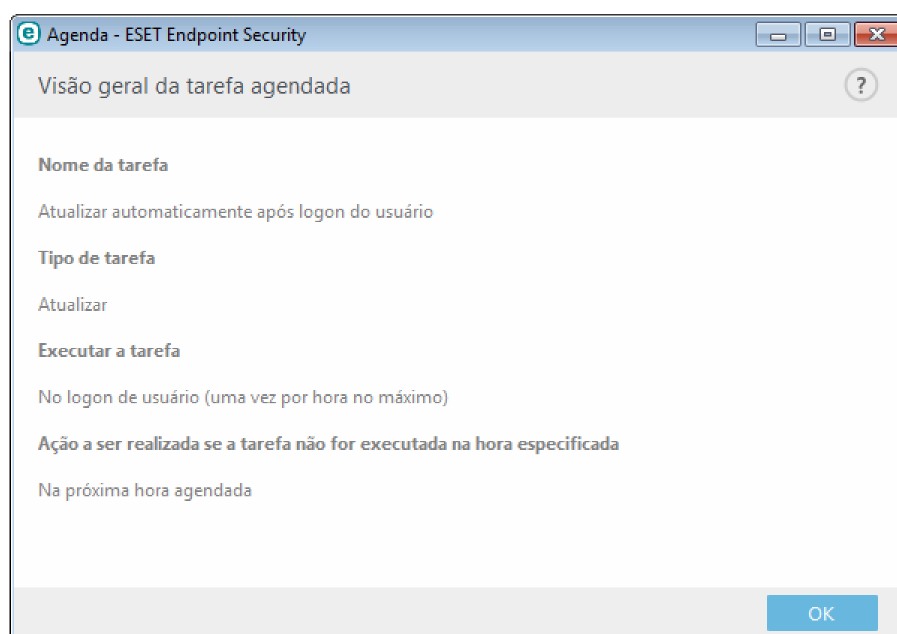
4. Ative a opção **Ativado** se quiser ativar a tarefa (você pode fazer isso posteriormente marcando/desmarcando a caixa de seleção na lista de tarefas agendadas), clique em **Avançar** e selecione uma das opções de tempo:

- **Uma vez** - A tarefa será realizada na data e hora predefinidas.
- **Repetidamente** - A tarefa será realizada no intervalo de tempo especificado.
- **Diariamente** - A tarefa será executada repetidamente todos os dias no horário especificado.
- **Semanalmente** - A tarefa será realizada na data e hora selecionadas.
- **Evento disparado** - A tarefa será realizada após um evento especificado.

5. Selecione **Pular tarefa quando estiver executando na bateria** para minimizar os recursos do sistema enquanto o laptop estiver em execução na bateria. A tarefa será realizada uma vez somente na data e hora especificadas nos campos **Execução de tarefas**. Se não foi possível executar a tarefa em um horário predefinido, você pode especificar quando ela será executada novamente:

- **Na próxima hora agendada**
- **O mais breve possível**
- **Imediatamente, se o tempo depois da última execução ultrapassar um valor específico** (o intervalo pode ser definido utilizando a caixa de rolagem **Tempo depois da última execução**)

Você pode revisar a tarefa agendada clicando com o botão direito do mouse em **Mostrar detalhes da tarefa**.



3.8.6.4 Estatísticas da proteção

Para exibir um gráfico de dados estatísticos relacionados aos módulos de proteção do ESET Endpoint Security, clique em **Ferramentas** > **Estatísticas da proteção**. Selecione o módulo de proteção desejado no menu suspenso **Estatísticas** para visualizar o gráfico e a legenda correspondentes. Se você passar o mouse sobre um item na legenda, somente os dados desse item serão exibidos no gráfico.

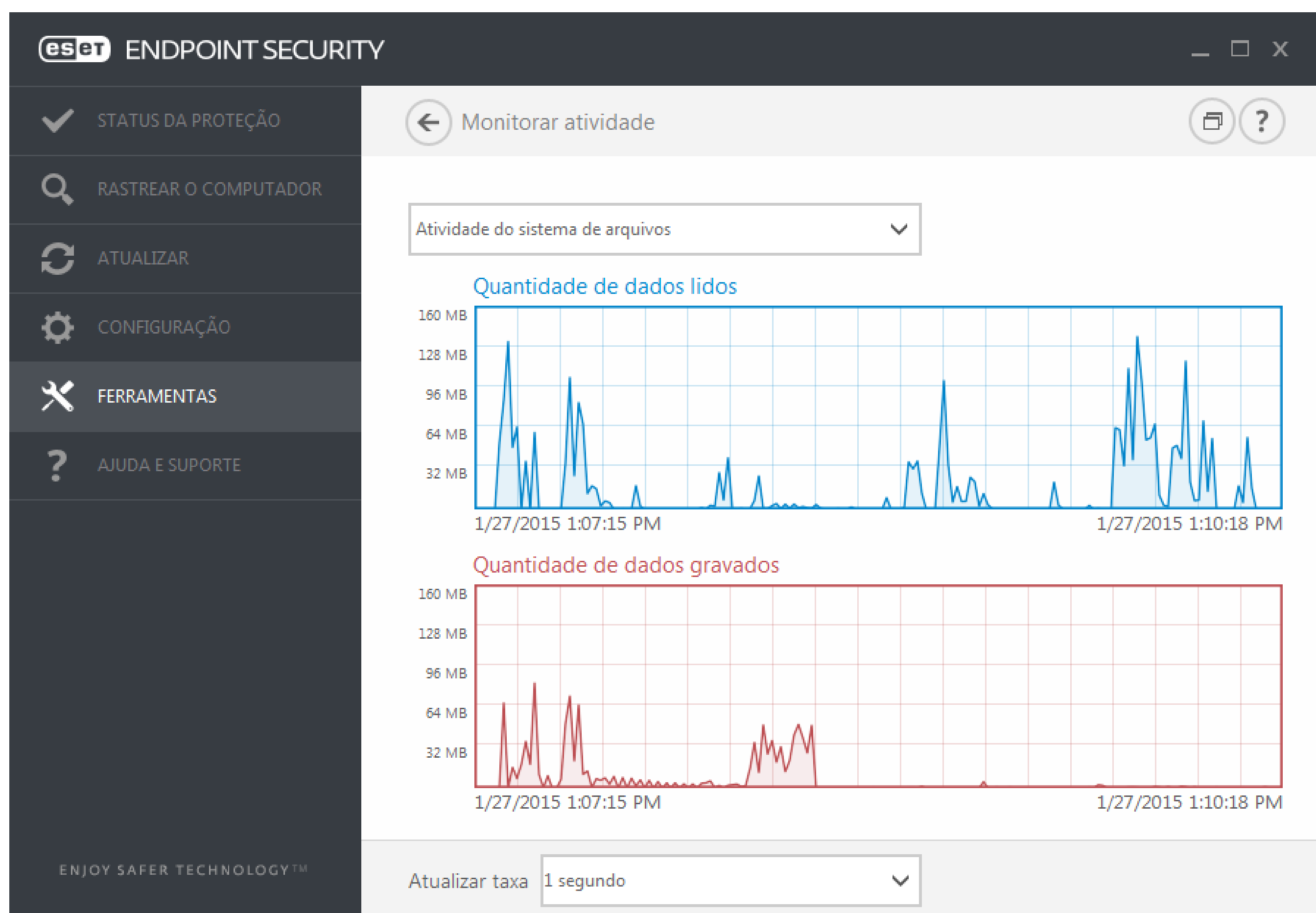
Os gráficos estatísticos a seguir estão disponíveis:

- **Proteção antivírus e antispyware** - Exibe o número de objetos infectados e limpos.
- **Proteção do sistema de arquivos** - Exibe apenas os objetos que foram lidos ou gravados no sistema de arquivos.
- **Proteção do cliente de email** - Exibe apenas os objetos que foram enviados ou recebidos pelos clientes de email.
- **Proteção antiphishing e de acesso à Web** - Exibe apenas os objetos obtidos por download pelos navegadores da web.
- **Proteção antispam do cliente de email** - Exibe o histórico das estatísticas de antispam desde a última inicialização.

Ao lado dos gráficos de estatísticas, você pode ver o número total de objetos rastreados, número de objetos infectados, número de objetos que foram limpos e o número de objetos que estão limpos. Clique em **Redefinir** para limpar informações de estatísticas ou clique em **Redefinir tudo** para limpar e remover todos os dados existentes.

3.8.6.5 Monitorar atividade

Para visualizar a **Atividade do sistema de arquivos** atual em forma gráfica, clique em **Ferramentas** > **Monitorar atividade**. Na parte inferior do gráfico, há uma linha do tempo que grava a atividade do sistema de arquivos em tempo real com base na duração do tempo selecionado. Para alterar a duração do tempo, selecione a partir do menu suspenso **Atualizar taxa**.



As opções disponíveis são:

- **Etapa: 1 segundo** - O gráfico é atualizado a cada segundo e a linha de tempo cobre os últimos 10 minutos.
- **Etapa: 1 minuto (últimas 24 horas)** - O gráfico é atualizado a cada minuto e a linha de tempo cobre as últimas 24 horas.
- **Etapa: 1 hora (último mês)** - O gráfico é atualizado a cada hora e a linha de tempo cobre o último mês.
- **Etapa: 1 hora (mês selecionado)** - O gráfico é atualizado a cada hora e a linha de tempo cobre os últimos X meses selecionados.

O eixo vertical do **Gráfico da atividade do sistema de arquivos** representa a quantidade de dados lidos (azul) e a quantidade de dados gravados (vermelho). Ambos os valores são fornecidos em KB (kilobytes)/MB/GB. Se você passar o mouse sobre os dados lidos ou sobre os dados gravados na legenda embaixo do gráfico, apenas os dados para esse tipo de atividade serão exibidos no gráfico.

Você também pode selecionar **Atividade de rede** a partir do menu suspenso. A exibição do gráfico e as opções da **Atividade do sistema de arquivos** e da **Atividade de rede** são as mesmas, exceto que a última exibe a quantidade de dados recebidos (azul) e a quantidade de dados enviados (vermelho).

3.8.6.6 ESET SysInspector

o ESET SysInspector é um aplicativo que inspeciona completamente o computador, coleta informações detalhadas sobre os componentes do sistema, como os drivers e aplicativos instalados, as conexões de rede ou entradas de registo importantes, e avalia o nível de risco de cada componente. Essas informações podem ajudar a determinar a causa do comportamento suspeito do sistema, que pode ser devido a incompatibilidade de software ou hardware ou infecção por malware.

A janela do SysInspector exibe as seguintes informações sobre os logs criados:

- **Hora** - A hora de criação do log.
- **Comentário** - Um comentário curto.
- **Usuário** - O nome do usuário que criou o log.
- **Status** - O status de criação do log.

As seguintes ações estão disponíveis:

- **Abrir** - Abre um relatório criado. Também é possível clicar com o botão direito do mouse em um determinado relatório e selecionar **Exibir** no menu de contexto.
- **Comparar** - Compara dois logs existentes.
- **Criar...** - Cria um novo log. Aguarde até que o ESET SysInspector tenha terminado (o status de relatório será exibido como Criado) antes de tentar acessar o relatório.
- **Excluir** - Exclui os relatórios selecionados da lista.

Os itens a seguir estão disponíveis no menu de contexto quando um ou mais relatórios são selecionados:

- **Mostrar** - Abre o log selecionado no ESET SysInspector (igual a clicar duas vezes em um log).
- **Comparar** - Compara dois relatórios existentes.
- **Criar...** - Cria um novo relatório. Aguarde até que o ESET SysInspector tenha terminado (o status de relatório será exibido como Criado) antes de tentar acessar o relatório.
- **Excluir tudo** - Exclui todos os logs.
- **Exportar...** - Exporta o log para um arquivo *.xml* ou *.xml* compactado.

3.8.6.7 ESET Live Grid

o ESET Live Grid é um sistema de avisos adiantado avançado composto de várias tecnologias baseadas na nuvem. Ele ajuda a detectar ameaças emergentes baseadas na reputação e melhora o desempenho de rastreamento através da lista de permissões. Informações sobre novas ameaças são enviadas em tempo real para a nuvem, o que permite que o ESET Malware Research Lab ofereça uma resposta oportuna e uniforme em todos os momentos. Os usuários podem verificar a reputação dos arquivos e dos processos em execução diretamente da interface do programa ou no menu de contexto, com informações adicionais disponíveis no ESET Live Grid. Ao instalar o ESET Endpoint Security, selecione uma das seguintes opções:

1. Você pode optar por não ativar o ESET Live Grid. Seu software não perderá nenhuma funcionalidade, mas, em alguns casos, o ESET Endpoint Security poderá responder mais devagar a novas ameaças do que a atualização do banco de dados de assinatura de vírus.
2. É possível configurar o ESET Live Grid para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça foi detectado. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar suas capacidades de detecção de ameaças.

O ESET Live Grid coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Por padrão, o ESET Endpoint Security é configurado enviar arquivos suspeitos ao Laboratório de vírus da ESET para análise detalhada. Os arquivos com certas extensões, como *.doc* ou *.xls*, são sempre excluídos. Você também pode adicionar outras extensões se houver arquivos específicos cujo envio você ou sua empresa desejam impedir.

O sistema de reputação do ESET Live Grid fornece lista de permissões e lista de proibições baseadas na nuvem. Para acessar configurações do ESET Live Grid, pressione **F5** para acessar a Configuração avançada e expanda **Ferramentas** > **ESET Live Grid**.

Ativar o sistema de reputação ESET Live Grid (recomendado) - O sistema de reputação do ESET Live Grid melhora a eficiência de soluções anti-malware da ESET ao comparar os arquivos rastreados com um banco de dados de itens na lista de proibições e permissões da nuvem.

Enviar estatísticas anônimas - Permite que a ESET colete informações sobre ameaças recém-detectadas como o nome, data e hora de detecção da ameaça, método de detecção e metadados associados, versão e configuração do produto, inclusive informações sobre seu sistema.

Enviar arquivos - Arquivos suspeitos, que se pareçam com ameaças e/ou arquivos com características ou comportamento incomuns são enviados à ESET para análise.

Selecione **Ativar registro em log** para criar um log de eventos para registrar os envios de arquivos e informações estatísticas. Isso vai permitir o registro no Log de eventos quando as estatísticas ou os arquivos são enviados.

Email de contato (opcional) - Seu email de contato pode ser incluído com qualquer arquivo suspeito e ser utilizado para que possamos entrar em contato com você se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

Exclusão - O Filtro de exclusões permite excluir determinados arquivos/pastas do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os arquivos relacionados nunca serão enviados aos laboratórios da ESET para análise, mesmo se incluírem um código suspeito. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, etc.). É possível adicioná-los à lista de arquivos excluídos, se desejar.

Se já tiver usado o ESET Live Grid antes e o tiver desativado, ainda pode haver pacotes de dados a enviar. Mesmo depois da desativação, tais pacotes serão enviados à ESET. Assim que todas as informações atuais forem enviadas, não serão criados pacotes adicionais.

3.8.6.8 Processos em execução

Os processos em execução exibem os programas ou processos em execução no computador e mantêm a ESET imediatamente e continuamente informada sobre novas infiltrações. O ESET Endpoint Security oferece informações detalhadas sobre os processos em execução a fim de proteger os usuários com a tecnologia ESET Live Grid ativada.

Nível de risco - Na maioria dos casos, o ESET Endpoint Security e a tecnologia ESET Live Grid atribui níveis de risco aos objetos (arquivos, processos, chaves de registro etc.), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 – Aceitável (verde) a 9 – Perigoso (vermelho).

Processo - Nome da imagem do programa ou processo em execução no computador. Você também pode usar o Gerenciador de tarefas do Windows para ver todos os processos que estão em execução no computador. O Gerenciador de tarefas pode ser aberto clicando-se com o botão direito em uma área vazia da barra de tarefas e, em seguida, clicando na opção **Ctrl+Shift+Esc** no teclado.

PID - É um ID de processos em execução em sistemas operacionais Windows.

OBSERVAÇÃO: Aplicativos conhecidos marcados como Aceitável (verde) são limpos definitivamente (lista de permissões) e serão excluídos do rastreamento, pois isso melhorará a velocidade do rastreamento sob demanda do computador ou da Proteção em tempo real do sistema de arquivos no computador.

Número de usuários - O número de usuários que utilizam um determinado aplicativo. Estas informações são reunidas pela tecnologia ESET Live Grid.

Hora da descoberta - Período de tempo a partir do momento em que o aplicativo foi detectado pela tecnologia ESET Live Grid.

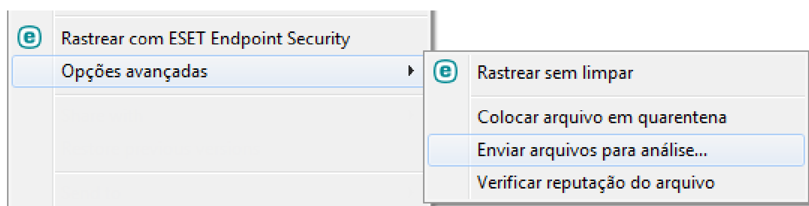
Observação: Quando um aplicativo é marcado com o nível de segurança Desconhecido (laranja), não é necessariamente um software malicioso. Geralmente, é apenas um aplicativo mais recente. Se você não estiver certo em relação ao arquivo, use o recurso enviar arquivo para análise para enviar o arquivo para o Laboratório de vírus da ESET. Se for detectado que o arquivo é um aplicativo malicioso, sua detecção será adicionada em uma das atualizações posteriores do banco de dados de assinatura de vírus.

Nome do aplicativo - O nome de um programa ou processo.

Ao clicar em um determinado aplicativo na parte inferior, as seguintes informações serão exibidas na parte inferior da janela:

- **Caminho** - Local de um aplicativo no computador.
- **Tamanho** - Tamanho do arquivo em kB (kilobytes) ou MB (megabytes).
- **Descrição** - Características do arquivo com base na descrição do sistema operacional.
- **Companhia** - Nome de processo do aplicativo ou do fornecedor.
- **Versão** - Informações do editor do aplicativo.
- **Produto** - Nome do aplicativo e/ou nome comercial.
- **Criado em** - Data e hora quando um aplicativo foi criado.
- **Modificado em** - Data e hora da última modificação de um aplicativo.

OBSERVAÇÃO: A reputação também pode ser verificada em arquivos que não agem como programas/processos em execução - marque os arquivos que deseja verificar, clique neles com o botão direito do mouse e, no menu de contexto, selecione **Opções avançadas** > **Verificar reputação do arquivo usando o ESET Live Grid**.



3.8.6.9 Conexões de rede

Na seção Conexões de rede, você pode ver uma lista de conexões ativas e pendentes. Isso o ajuda a controlar todos os aplicativos que estabelecem conexões de saída.

A primeira linha exibe o nome do aplicativo e a velocidade de transferência dos dados. Para ver a lista de conexões feitas pelo aplicativo (bem como informações mais detalhadas), clique em **+**.

Colunas

Aplicativo/IP local - Nome do aplicativo, endereços IP locais e portas de comunicação.

IP remoto - Endereço IP e número de porta de um computador remoto específico.

Protocolo - Protocolo de transferência utilizado.

Velocidade de entrada/de saída - A velocidade atual dos dados de saída e entrada.

Enviados/Recebidos - Quantidade de dados trocados na conexão.

Mostrar detalhes - Escolha esta opção para exibir informações detalhadas sobre a conexão selecionada.

Selecione um aplicativo ou endereço IP na tela Conexões de rede e clique nele com o botão direito do mouse para exibir o menu de contexto com a seguinte estrutura:

Solucionar nomes de host - Se possível, todos os endereços de rede serão exibidos no formato DNS, não no formato de endereço IP numérico.

Exibir somente conexões TCP - A lista só exibe conexões que pertencem ao pacote de protocolo TCP.

Mostrar conexões de escuta - Selecione essa opção para exibir somente conexões em que não haja comunicação atualmente estabelecida, mas o sistema tenha aberto uma porta e esteja aguardando por conexão.

Mostrar conexões no computador - Selecione essa opção para mostrar somente conexões nas quais o lado remoto é um sistema local - as chamadas conexões de *localhost*.

Clique com o botão direito do mouse em uma conexão para visualizar as opções adicionais, que incluem:

Negar comunicação para a conexão - Encerra a comunicação estabelecida. Essa opção só fica disponível depois que você clica em uma conexão ativa.

Velocidade de atualização - Escolha a frequência para atualizar as conexões ativas.

Atualizar agora - Recarrega a janela Conexões de rede.

As opções a seguir só ficam disponíveis depois que você clica em um aplicativo ou processo, não em uma conexão ativa:

Negar temporariamente comunicação para o processo - Rejeita as atuais conexões de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção Regras e zonas.

Permitir temporariamente comunicação para o processo - Permite as conexões atuais de determinado aplicativo. Se uma nova conexão for estabelecida, o firewall utilizará uma regra predefinida. Uma descrição das configurações pode ser encontrada na seção Regras e zonas.

3.8.6.10 Envio de amostras para análise

A caixa de diálogo de envio de amostras permite enviar um arquivo ou site para a ESET para fins de análise e pode ser acessada em **Ferramentas** > **Enviar amostra para análise**. Se você detectar um arquivo com comportamento suspeito no seu computador ou um site suspeito na internet, poderá enviá-lo para o Laboratório de vírus da ESET para análise. Se for detectado que o arquivo é um aplicativo ou site malicioso, sua detecção será adicionada em uma das atualizações posteriores.

Como alternativa, você pode enviar o arquivo por email. Se for esta sua opção, compacte o(s) arquivo(s) usando WinRAR/ZIP, proteja o arquivo com a senha "infected" (infectado) e envie-o para samples@eset.com. Lembre-se de incluir uma linha de assunto clara e o máximo de informações possível sobre o arquivo (por exemplo, o site do qual fez o download).

OBSERVAÇÃO: antes de enviar uma amostra para a ESET, certifique-se de que ele atenda a um ou mais dos seguintes critérios:
- o arquivo ou site não foi detectado
- o arquivo ou site foi detectado incorretamente como uma ameaça

Você não receberá uma resposta, a não ser que mais informações sejam necessárias para a análise.

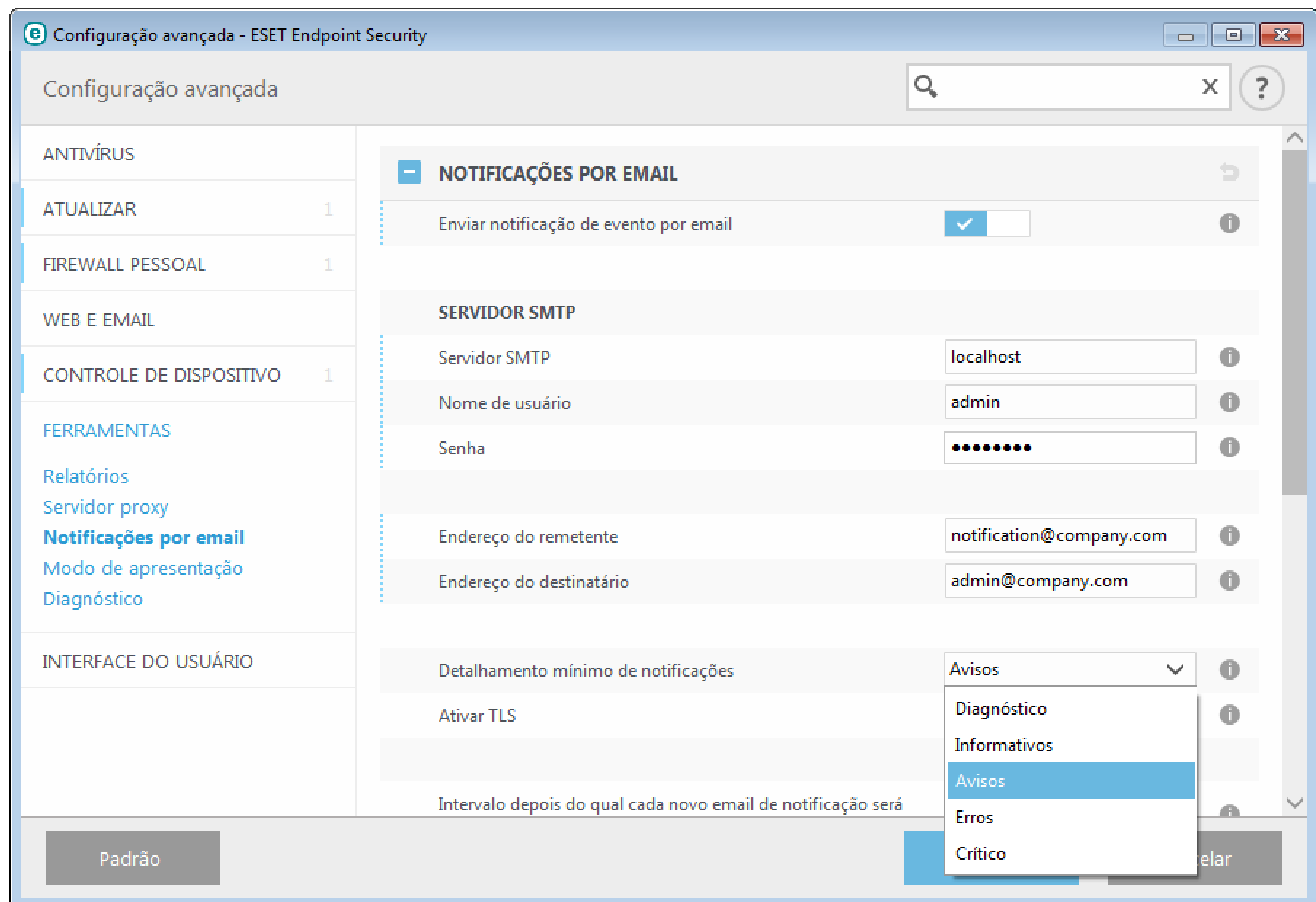
Selecione a descrição no menu suspenso **Motivo para envio da amostra** mais adequada à sua mensagem:
- **Arquivo suspeito**
- **Site suspeito** (um site que está infectado por algum malware),
- **Arquivo falso positivo** (arquivo que é detectado como uma infecção, mas que não está infectado),
- **Site falso positivo**
- **Outros**

Arquivo/Site - O caminho do arquivo ou site que você pretende enviar.

Email de contato - O email de contato é enviado junto com arquivos suspeitos para a ESET e pode ser utilizado para contatar você se informações adicionais sobre os arquivos suspeitos forem necessárias para análise. É opcional inserir um email de contato. Você não obterá uma resposta da ESET, a menos que mais informações sejam necessárias, pois a cada dia os nossos servidores recebem milhares de arquivos, o que torna impossível responder a todos os envios.

3.8.6.11 Notificações por email

O ESET Endpoint Security poderá enviar automaticamente e-mails de notificação se um evento com o nível de detalhamento selecionado ocorrer. Ative **Enviar notificações de evento por email** para ativar notificações por e-mail.



Servidor SMTP

Servidor SMTP - O servidor SMTP usado para o envio de notificações. (por exemplo *smtp.provider.com:587*, a porta pré-definida é 25).

OBSERVAÇÃO: Os servidores SMTP com criptografia TLS são compatíveis com o ESET Endpoint Security.

Nome de usuário e **senha** - Se o servidor SMTP exigir autenticação, esses campos devem ser preenchidos com nome de usuário e senha válidos para conceder acesso ao servidor SMTP.

Endereço do remetente - Esse campo especifica o endereço do remetente que será exibido no cabeçalho dos

emails de notificação.

Endereço do destinatário - Esse campo especifica o endereço do destinatário que será exibido no cabeçalho dos emails de notificação.

No menu suspenso **Detalhamento mínimo de notificações**, é possível selecionar o nível de gravidade inicial das notificações a serem enviadas.

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas como eventos de rede fora do padrão, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso (o Anti-Stealth não está sendo executado corretamente ou a atualização falhou).
- **Erros** - Erros (proteção de documentos não iniciada) e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos como erro ao iniciar a proteção antivírus ou sistema infectado.

Ativar TLS - Ativa o envio de mensagens de alerta e notificação compatíveis com a criptografia TLS.

Intervalo depois do qual cada novo email de notificação será enviado (min) - Intervalo em minutos depois do qual cada nova notificação será enviada por email. Se configurar este valor como 0, as notificações serão enviadas imediatamente.

Enviar cada notificação em um email separado - Quando ativado, o destinatário receberá um novo email para cada notificação individual. Isso pode resultar em um grande número de emails recebidos em um curto período de tempo.

Formato de mensagem

Formato de mensagens de eventos - O formato de mensagens de eventos que são exibidas em computadores remotos.

Formato das mensagens de aviso de ameaça - Mensagens de alerta de ameaça e notificação têm um formato padrão predefinido. Não aconselhamos alterar esse formato. No entanto, em algumas circunstâncias (por exemplo, se você tiver um sistema de processamento de email automatizado), você pode precisar alterar o formato da mensagem.

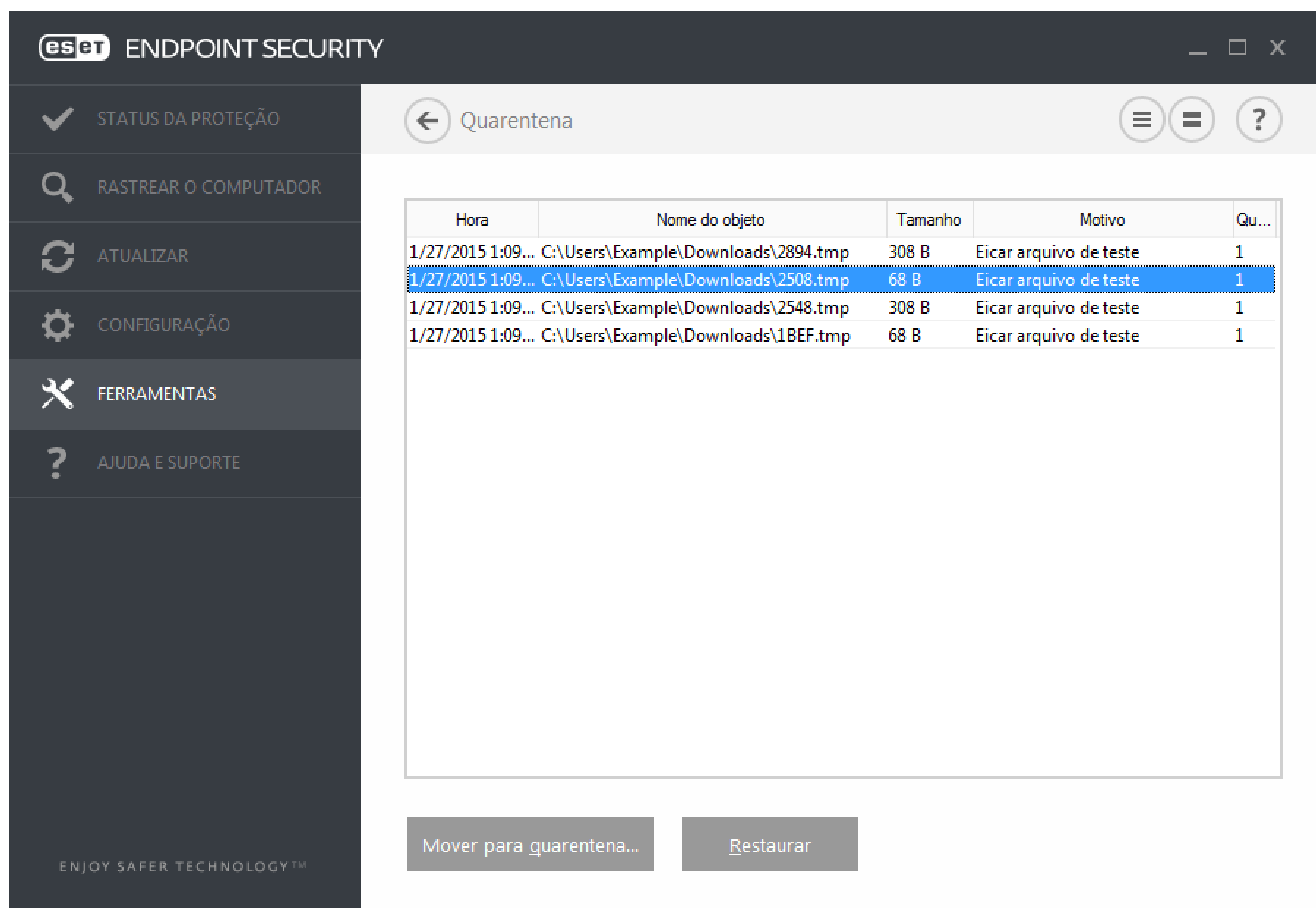
Utilizar caracteres do alfabeto local - Converte uma mensagem de email na codificação de caracteres ANSI com base nas configurações regionais do Windows (por exemplo, windows-1250). Se você deixar essa opção desmarcada, uma mensagem será convertida e codificada em ACSII de 7 bits (por exemplo, "á" será alterada para "a" e um símbolo desconhecido para "?").

Utilizar codificações de caracteres locais - A origem da mensagem de email será codificada para o formato Quoted-printable (QP) que usa caracteres ASCII e pode transmitir caracteres nacionais especiais por email no formato de 8 bits (áéíóú).

3.8.6.12 Quarentena

A principal função da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Endpoint Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo rastreador de antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de vírus da ESET para análise.



Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e a hora da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, objeto adicionado pelo usuário) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças).

Colocação de arquivos em quarentena

o ESET Endpoint Security coloca automaticamente os arquivos excluídos em quarentena (se você não desativou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando em **Quarentena**. O arquivo original será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela **Quarentena** e selecione **Quarentena**.

Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Para restaurar um arquivo na quarentena, clique com o botão direito na janela Quarentena e selecione **Restaurar** no menu de contexto. Se um arquivo for marcado como um Aplicativo potencialmente não desejado, **Restaurar e excluir do rastreamento** também estará disponível. O menu de contexto também contem a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

Excluindo da quarentena - Clique com o botão direito em um determinado item e selecione **Excluir da quarentena**, ou selecione o item que você quer excluir e pressione **Excluir** no seu teclado. Também é possível selecionar vários

itens e excluí-los juntos.

OBSERVAÇÃO: Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo do rastreamento após restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

Envio de um arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi determinado incorretamente como uma ameaça e colocado em quarentena, envie o arquivo para o Laboratório de vírus da ESET. Para enviar um arquivo diretamente da quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

3.8.6.13 Microsoft Windows Update

O recurso de atualização do Windows é um componente importante de proteção de usuários contra software malicioso. Por esse motivo, é extremamente importante manter as atualizações do Microsoft Windows em dia, instalando-as assim que forem disponibilizadas. O ESET Endpoint Security o notificará sobre as atualizações ausentes de acordo com o nível que você especificar. Os seguintes níveis estão disponíveis:

- **Nenhuma atualização** - Nenhuma atualização de sistema será proposta para download.
- **Atualizações opcionais** - Atualizações marcadas como de baixa prioridade e superiores serão propostas para download.
- **Atualizações recomendadas** - Atualizações marcadas como comuns e superiores serão propostas para download.
- **Atualizações importantes** - Atualizações marcadas como importantes e superiores serão propostas para download.
- **Atualizações críticas** - Apenas atualizações críticas serão propostas para download.

Clique em **OK** para salvar as alterações. A janela Atualizações do sistema será exibida depois da verificação do status com o servidor de atualização. Assim, as informações sobre atualização de sistema podem não estar disponíveis imediatamente após as alterações serem salvas.

3.8.7 Interface do usuário

A seção **Interface do usuário** permite configurar o comportamento da GUI (Graphical User Interface, interface gráfica do usuário) do programa.

Usando a ferramenta Elementos da interface do usuário, é possível ajustar a aparência visual do programa e os efeitos usados.

Para obter a máxima segurança do seu software de segurança, você pode evitar quaisquer alterações não autorizadas usando a ferramenta Configuração de acesso.

Ao configurar Alertas e notificações, você pode alterar o comportamento de alertas de ameaças detectadas e notificações do sistema. Esses recursos podem ser personalizados de acordo com suas necessidades.

Se você escolher não exibir algumas notificações, elas serão exibidas na área **Elementos da interface do usuário** > **Status de aplicativo**. Aqui é possível verificar o status ou, alternativamente, impedir a exibição dessas notificações.

A Integração do menu de contexto é exibida após um clique com o botão direito do mouse no objeto selecionado. Utilize essa ferramenta para integrar os elementos de controle do ESET Endpoint Security no menu de contexto.

O Modo de apresentação é útil para usuários que pretendem trabalhar com um aplicativo, sem serem interrompidos por janelas pop-up, tarefas agendadas ou quaisquer componentes que possam carregar o processador e a RAM.

3.8.7.1 Elementos da interface do usuário

As opções de configuração da interface do usuário no ESET Endpoint Security permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções de configuração são acessíveis na ramificação **Interface do usuário** > **Elementos da interface do usuário** da árvore Configuração avançada do ESET Endpoint Security.

Na seção **Elementos da interface do usuário**, é possível ajustar o ambiente de trabalho. Use o menu suspenso **Modo de início de GUI** para selecionar entre os seguintes modos de início da interface gráfica do usuário (GUI):

Completo - Toda a interface gráfica do usuário será exibida.

Mínimo - A interface gráfica do usuário está disponível, mas apenas as notificações são exibidas ao usuário.

Manual - Nenhuma notificação ou alerta será exibido.

Silencioso - Nem a interface gráfica do usuário nem as notificações e alertas serão exibidos. Este modo pode ser útil em situações onde você precisa preservar os recursos do sistema. O modo silencioso pode ser iniciado somente pelo Administrador.

OBSERVAÇÃO: Quando o modo de início de interface gráfica do usuário mínima estiver selecionado e seu computador for reiniciado, serão exibidas notificações mas não a interface gráfica. Para voltar ao modo de interface gráfica do usuário completa, execute a interface gráfica do usuário no menu Iniciar em **Todos os programas** > **ESET** > ESET Endpoint Security como um administrador, ou faça isso através do ESET Remote Administrator usando uma política.

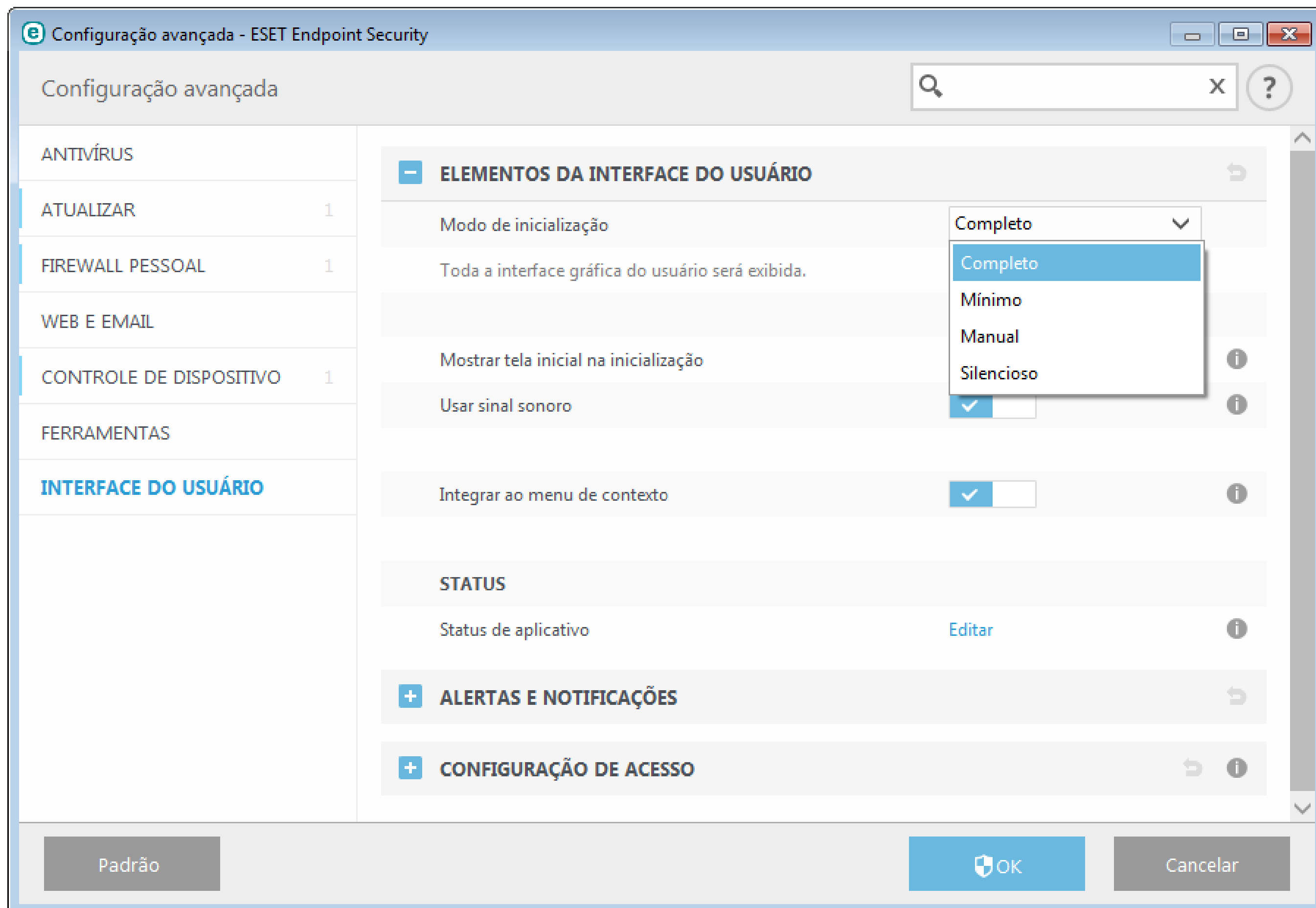
Se desejar desativar a tela inicial do ESET Endpoint Security, desmarque a opção **Mostrar tela inicial na inicialização**.

Se você quiser que o ESET Endpoint Security reproduza um som quando ocorrerem eventos importantes durante um rastreamento, por exemplo quando uma ameaça é descoberta ou quando a verificação for concluída, selecione **Usar sinal sonoro**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET Endpoint Security no menu de contexto.

Status

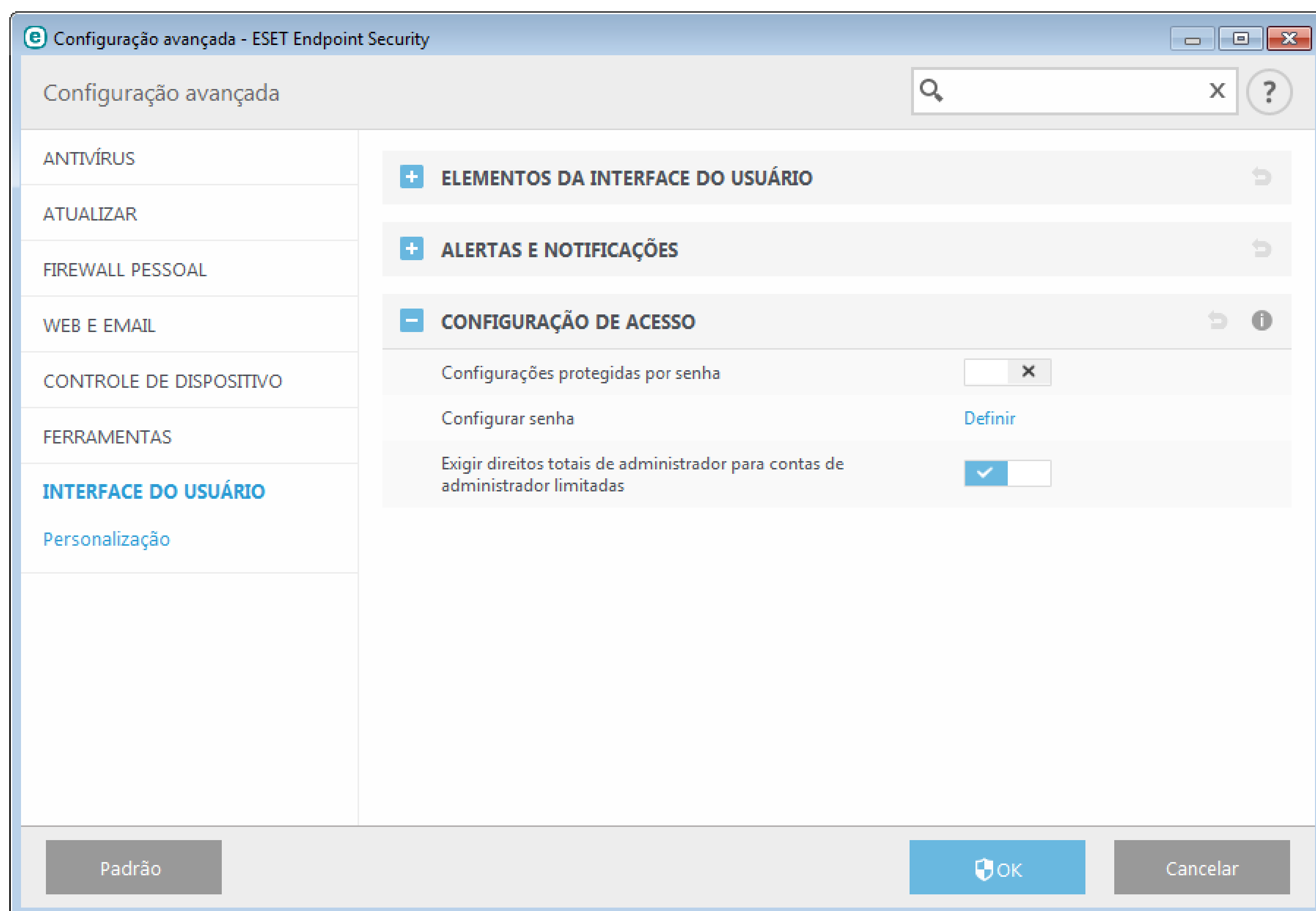
Status de aplicativo - Clique no botão **Editar** para gerenciar (desativar) status que são exibidos no painel **Status da proteção** no menu principal.



Configuração avançada - ESET Endpoint Security
Configuração avançada
ANTIVÍRUS
ATUALIZAR 1
FIREWALL PESSOAL 1
WEB E EMAIL
CONTROLE DE DISPOSITIVO 1
FERRAMENTAS
INTERFACE DO USUÁRIO
ELEMENTOS DA INTERFACE DO USUÁRIO
Modo de inicialização
Completo
Toda a interface gráfica do usuário será exibida.
Completo
Mínimo
Manual
Silencioso
Mostrar tela inicial na inicialização
Usar sinal sonoro
Integrar ao menu de contexto
STATUS
Status de aplicativo
Editar
ALERTAS E NOTIFICAÇÕES
CONFIGURAÇÃO DE ACESSO
Padrão
OK
Cancelar

3.8.7.2 Configuração do acesso

Para fornecer segurança máxima ao seu sistema, é fundamental que o ESET Endpoint Security seja configurado corretamente. Qualquer alteração não qualificada pode resultar em perda de dados importantes. Para evitar modificações não autorizadas, os parâmetros de configuração do ESET Endpoint Security podem ser protegidos por senha. As configurações de proteção da senha estão localizadas em **Configuração avançada** (F5) sob **Configuração de acesso** > **Interface do usuário**.



Configurações protegidas por senha - Indica as configurações com senha. Clique para abrir a janela Configuração de senha.

Para definir uma senha para proteger os parâmetros de configuração, clique em **Definir**.

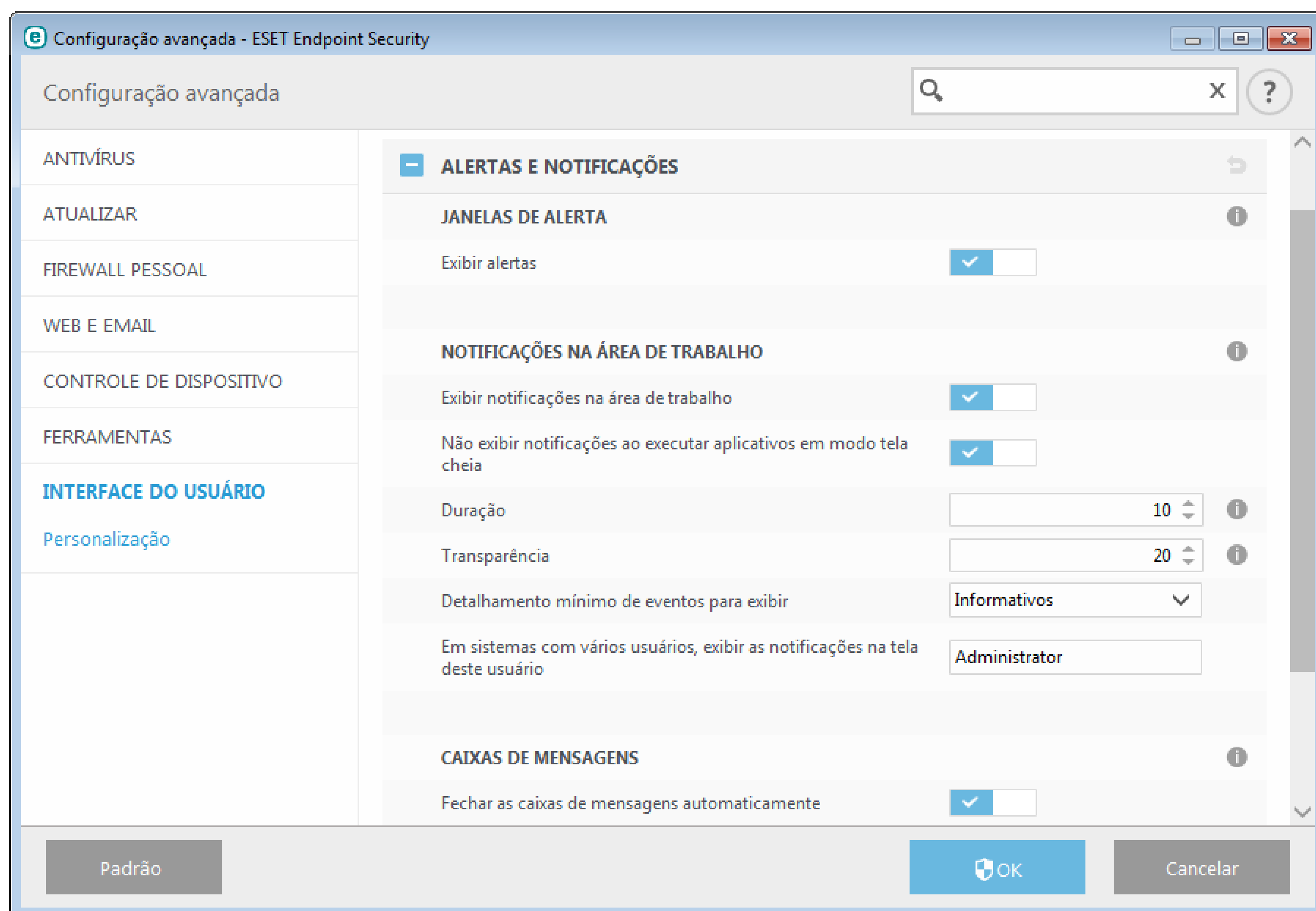
Exigir direitos totais de administrador para contas de administrador limitadas - Ative essa opção para solicitar que o usuário atual (se ele não tiver direitos de administrador) digite o nome de usuário e a senha de administrador quando modificar determinados parâmetros do sistema (semelhante ao UAC no Windows Vista). As modificações incluem a desativação dos módulos de proteção ou a desativação do firewall.

Apenas vara Windows XP:

Exigir direitos de administrador (sistema sem suporte UAC) - Ative esta opção para que o ESET Endpoint Security peça as credenciais do administrador.

3.8.7.3 Alertas e notificações

A seção **Alertas e notificações** em **Interface do usuário** permite que você configure como os alertas de ameaças e as notificações do sistema (por exemplo, mensagens de atualização bem-sucedida) são tratados no ESET Endpoint Security. Você também pode definir a hora e o nível de transparência das notificações da bandeja do sistema (aplica-se somente aos sistemas compatíveis com notificações na bandeja do sistema).



Janelas de alerta

Desativar a opção **Exibir alertas** cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

Mensagens dentro do produto

Exibir mensagens de marketing - As mensagens dentro do produto foram feitas para informar os usuários ESET sobre novidades e outras comunicações. Desative esta opção se não quiser receber mensagens de marketing.

Notificações na área de trabalho

As notificações na área de trabalho e as dicas de balão são apenas informativas e não requerem interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar as notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Ative a opção **Não exibir notificações ao executar aplicativos em modo tela cheia** para suprimir todas as notificações não interativas. Opções mais detalhadas, como o tempo de exibição e a transparência da janela de notificação, podem ser modificadas a seguir.

O menu suspenso **Detalhamento mínimo de eventos para exibir** permite selecionar o nível de gravidade de alertas e notificações a serem exibidos. As opções disponíveis são:

- **Diagnóstico** - Registra informações necessárias para ajustar o programa e todos os registros mencionados anteriormente.
- **Informativos** - Registra as mensagens informativas, incluindo as mensagens de atualizações bem-sucedidas e todos os registros mencionados anteriormente.
- **Avisos** - Registra mensagens de erros críticos e de aviso.
- **Erros** - Erros como "Erro ao fazer download de arquivo" e erros críticos serão registrados.
- **Crítico** - Registra somente os erros críticos (como erro ao iniciar a proteção antivírus , firewall integrado, etc...).

O último recurso dessa seção permite configurar o destino das notificações em um ambiente com vários usuários. O campo **Em sistemas com vários usuários, exibir as notificações na tela deste usuário** especifica um usuário que receberá notificações do sistema e outras notificações sobre os sistemas, permitindo que diversos usuários se conectem ao mesmo tempo. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Esta opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

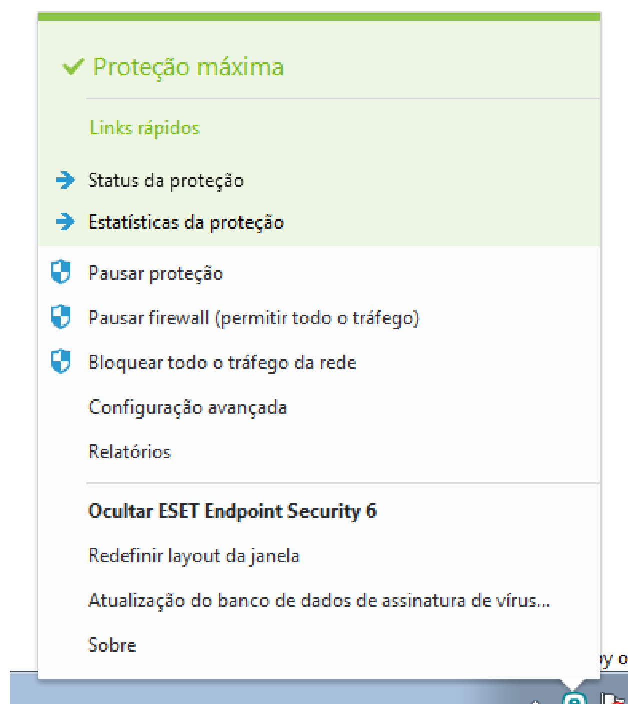
Caixas de mensagens

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente**. Se não forem fechadas manualmente, as janelas de alertas serão fechadas automaticamente após o período de tempo especificado expirar.

Mensagens de confirmação - Mostra a você uma lista de mensagens de confirmação que você pode selecionar para serem exibidas ou não.

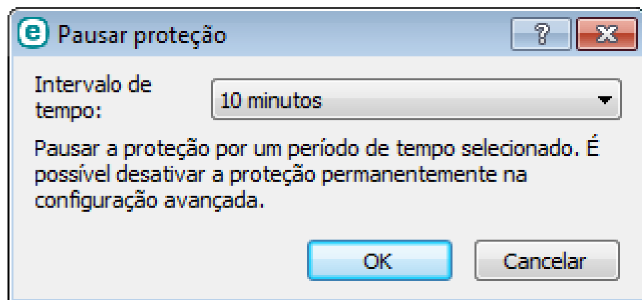
3.8.7.4 Ícone da bandeja do sistema

Estão disponíveis alguns dos recursos e opções de configuração mais importantes clicando com o botão direito do mouse no ícone da bandeja do sistema.



Bloquear o tráfego de rede - O firewall pessoal bloqueará todo o tráfego de entrada e saída da rede e da Internet.

Pausar proteçãoe - Exibe a caixa de diálogo de confirmação que desativa a Proteção antivírus e antispyware, que protege contra ataques controlando arquivos e a comunicação via web e por emails.



O menu suspenso **Intervalo de tempo** representa o período de tempo em que a proteção antivírus e antispyware será desativada.

Pausar firewall (permitir todo o tráfego) - Alterna o firewall para o estado inativo. Para obter mais informações, consulte Rede.

Bloquear todo o tráfego da rede - Bloqueia todo o tráfego da rede. É possível reativar clicando em **Parar de bloquear todo o tráfego de rede**.

Configuração avançada - Selecione essa opção para acessar a árvore **Configuração avançada**. Você também pode acessar a Configuração avançada pressionando a tecla F5 ou acessando **Configuração** > **Configuração avançada**.

Relatórios - Os relatórios contêm informações sobre todos os eventos importantes do programa que ocorreram e fornece uma visão geral das ameaças detectadas.

Ocultar ESET Endpoint Security - Oculta a janela do ESET Endpoint Security da tela.

Redefinir layout da janela - Redefine a janela do ESET Endpoint Security para seu tamanho e posição padrão na tela.

Atualização do banco de dados de assinatura de vírus - Inicia a atualização do banco de dados de assinatura de vírus para garantir seu nível de proteção em relação ao código malicioso.

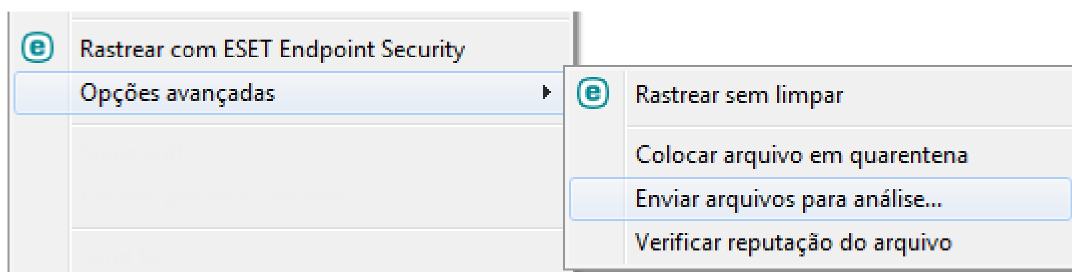
Sobre - As informações do sistema fornecem detalhes sobre a versão instalada do ESET Endpoint Security e os componentes do programa instalados, bem como a data de expiração de sua licença. Informações sobre seu sistema operacional e recursos do sistema podem ser encontradas no final da página.

3.8.7.5 Menu de contexto

O menu de contexto é exibido após um clique com o botão direito do mouse em um objeto (arquivo). O menu relaciona todas as ações que você pode realizar em um objeto.

É possível integrar os elementos de controle do ESET Endpoint Security no menu de contexto. A opção de configuração está disponível para essa funcionalidade na árvore Configuração avançada em **Interface do usuário** > **Elementos da interface do usuário**.

Integrar ao menu de contexto - Integra os elementos de controle do ESET Endpoint Security no menu de contexto.



3.9 Usuário avançado

3.9.1 Gerenciador de perfil

O gerenciador de perfil é usado em duas seções no ESET Endpoint Security - **Rastreamento sob demanda do computador** e **Atualizar**.

Rastreamento sob demanda do computador

Os seus parâmetros de rastreamento favoritos podem ser salvos para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, abra a janela Configuração avançada (F5) e clique em **Antivírus** > **Rastreamento sob demanda do computador** e em **Editar** ao lado de **Lista de perfis**. O menu suspenso **Perfil selecionado** que lista os perfis de rastreamento existentes. Para ajudar a criar um perfil de rastreamento que atenda às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a **Limpeza rígida**. Digite o nome do novo perfil na janela **Gerenciador de perfil** e clique em **Adicionar**. Selecione seu novo perfil do menu suspenso **Perfil selecionado** e ajuste os parâmetros restantes para atender aos seus requisitos e clique em **OK** para salvar seu novo perfil.

Atualizar

O editor de perfil na seção de configuração da Atualização permite que os usuários criem novos perfis de atualização. Crie e use os seus próprios perfis personalizados (isto é, outros que não sejam o padrão **Meu perfil**) somente se o seu computador usar diversos modos de conexão com os servidores de atualização.

Por exemplo, um laptop que normalmente se conecta ao servidor local (Mirror) na rede local, mas faz os downloads das atualizações diretamente dos servidores de atualização da ESET quando está desconectado da rede local (em viagem de negócios, por exemplo) pode usar dois perfis: o primeiro para conectar ao servidor local; o segundo para conectar aos servidores da ESET. Quando esses perfis estiverem configurados, navegue até **Ferramentas** > **Agenda** e edite os parâmetros da tarefa de atualização. Designe um perfil como primário e outro como secundário.

Perfil selecionado - O perfil de atualização atualmente usado. Para mudar, escolha um perfil no menu suspenso.

Lista de perfis - Crie novos perfis de atualização ou remova os existentes.

3.9.2 Diagnóstico

O diagnóstico fornece despejos de memória de aplicativos dos processos da ESET (por exemplo, *ekrn*). Se um aplicativo falhar, um despejo será gerado. Isso poderá ajudar os desenvolvedores a depurar e a corrigir os problemas do ESET Endpoint Security. Clique no menu suspenso ao lado de **Tipo de despejo** e selecione uma das três opções disponíveis:

- Selecione **Desativar** (padrão) para desativar esse recurso.
- **Mini** - Registra o menor conjunto de informações úteis que podem ajudar a identificar porque o aplicativo parou inesperadamente. Este tipo de arquivo de despejo pode ser útil quando o espaço é limitado, no entanto, devido às informações limitadas incluídas, os erros que não foram causados diretamente pelo encadeamento que estava em execução no momento em que o problema ocorreu, podem não ser descobertos por uma análise desse arquivo.
- **Completo** - Registra todo o conteúdo da memória do sistema quando o aplicativo para inesperadamente. Um despejo de memória completo pode conter dados de processos que estavam em execução quando o despejo de memória foi coletado.

Ativar registro em relatório avançado de Filtragem de protocolo - Registrar todos os dados passando pelo

mecanismo de Filtragem de protocolo em formato PCAP para ajudar os desenvolvedores a diagnosticar e solucionar problemas relacionados a Filtragem de protocolo.

Os arquivos de relatório podem ser encontrados em:
C:\ProgramData\ESET\ESET Smart Security\Diagnostics no Windows Vista e versões posteriores ou *C:\Documentos e configurações\Todos os usuários\...* em versões anteriores do Windows.

Diretório de destino – Diretório no qual o despejo durante a falha será gerado.

Abrir pasta de diagnóstico - Clique em **Abrir** para abrir esse diretório em uma nova janela do *Windows explorer*.

3.9.3 Importar e exportar configurações

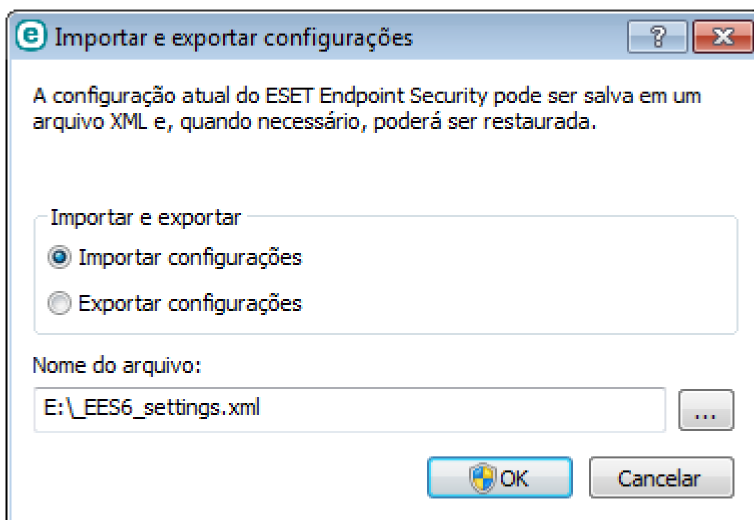
Você pode importar ou exportar seu arquivo de configuração .xml personalizado do ESET Endpoint Security do menu **Configuração**.

A importação e a exportação dos arquivos de configuração serão úteis caso precise fazer backup da configuração atual do ESET Endpoint Security para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais em diversos sistemas. Os usuários podem importar facilmente um arquivo *.xml* para transferir essas configurações.

A importação de uma configuração é muito fácil. Na janela principal do programa, clique em **Configuração** > **Importar/exportar configurações** e selecione a opção **Importar configurações**. Digite o nome do arquivo de configuração ou clique no botão **...** para procurar o arquivo de configuração que deseja importar.

As etapas para exportar uma configuração são muito semelhantes. Na janela principal do programa, clique em **Configuração** > **Importar/exportar configurações**. Selecione a opção **Exportar configurações** e insira o nome de arquivo do arquivo de configuração (ou seja, *export.xml*). Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

OBSERVAÇÃO: Você pode encontrar um erro ao exportar configurações se não tiver direitos suficientes para gravar o arquivo exportado no diretório especificado.



3.9.4 Linha de comando

O módulo antivírus do ESET Endpoint Security pode ser iniciado pela linha de comando – manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat"). Uso para o rastreamento por linha de comando da ESET:

```
ecls [OPTIONS..] FILES..
```

Os seguintes parâmetros e chaves podem ser utilizados ao executar o scanner sob demanda na linha de comando:

Opções

/base-dir=PASTA	carregar módulos da PASTA
/quar-dir=PASTA	PASTA de quarentena
/exclude=MÁSCARA	excluir arquivos que correspondem à MÁSCARA do rastreamento

/subdir	rastrear subpastas (padrão)
/no-subdir	não rastrear subpastas
/max-subdir-level=NÍVEL	subnível máximo de pastas dentro de pastas para rastrear
/symlink	seguir links simbólicos (padrão)
/no-symlink	ignorar links simbólicos
/ads	rastrear ADS (padrão)
/no-ads	não rastrear ADS
/log-file=ARQUIVO	registrar o relatório em ARQUIVO
/log-rewrite	substituir arquivo de saída (padrão - acrescentar)
/log-console	registrar saída para console (padrão)
/no-log-console	não registrar saída para console
/log-all	também registrar arquivos limpos
/no-log-all	não registrar arquivos limpos (padrão)
/aind	mostrar indicador de atividade
/auto	rastrear e limpar automaticamente todos os discos locais

Opções do scanner

/files	rastrear arquivos (padrão)
/no-files	não rastrear arquivos
/memory	rastrear memória
/boots	rastrear setores de inicialização
/no-boots	não rastrear setores de inicialização (padrão)
/arch	rastrear arquivos compactados (padrão)
/no-arch	não rastrear arquivos compactados
/max-obj-size=TAMANHO	rastrear apenas arquivos com menos de TAMANHO megabytes (padrão 0 = sem limite)
/max-arch-level=NÍVEL	subnível máximo de arquivos dentro de arquivos (arquivos aninhados) para rastrear
/scan-timeout=LIMITE	rastrear arquivos pelo LIMITE máximo de segundos
/max-arch-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado se eles tiverem menos de TAMANHO (padrão 0 = sem limite)
/max-sfx-size=TAMANHO	rastrear apenas os arquivos em um arquivo compactado de auto-extração se eles tiverem menos de TAMANHO megabytes (padrão 0 = sem limite)
/mail	rastrear arquivos de email (padrão)
/no-mail	não rastrear arquivos de email
/mailbox	rastrear caixas de correio (padrão)
/no-mailbox	não rastrear caixas de correio
/sfx	rastrear arquivos compactados de auto-extração (padrão)
/no-sfx	não rastrear arquivos compactados de auto-extração
/rtp	rastrear empacotadores em tempo real (padrão)
/no-rtp	não rastrear empacotadores em tempo real
/unsafe	rastrear por aplicativos potencialmente inseguros
/no-unsafe	não rastrear por aplicativos potencialmente inseguros (padrão)
/unwanted	rastrear por aplicativos potencialmente indesejados
/no-unwanted	não rastrear por aplicativos potencialmente indesejados (padrão)
/suspicious	rastrear aplicativos suspeitos (padrão)
/no-suspicious	não rastrear aplicativos suspeitos
/pattern	usar assinaturas (padrão)
/no-pattern	não usar assinaturas
/heur	ativar heurística (padrão)
/no-heur	desativar heurística
/adv-heur	ativar heurística avançada (padrão)
/no-adv-heur	desativar heurística avançada
/ext=EXTENSÕES	verificar somente EXTENSÕES delimitadas por dois pontos
/ext-exclude=EXTENSÕES	excluir do rastreamento EXTENSÕES delimitadas por dois pontos

/clean-mode=MODO	utilizar MODO de limpeza para objetos infectados As opções disponíveis são: • none (nenhuma) - não ocorrerá nenhuma limpeza automática. • standard (padrão) - o ecls.exe tentará limpar ou excluir automaticamente os arquivos infectados. • strict (rígida) - o ecls.exe tentará limpar ou excluir automaticamente todos os arquivos infectados sem intervenção do usuário (você não será avisado antes de os arquivos serem excluídos). • rigorous (rigorosa) - o ecls.exe excluirá arquivos sem tentar limpá-los, independentemente de quais arquivos sejam. • delete (excluir) - o ecls.exe excluirá arquivos sem tentar limpá-los, mas não excluirá arquivos importantes, como arquivos do sistema Windows.
/quarantine	copiar arquivos infectados para Quarentena (completa a ação realizada enquanto ocorre a limpeza)
/no-quarantine	não copiar arquivos infectados para Quarentena

Opções gerais

/help	mostrar ajuda e sair
/version	mostrar informações de versão e sair
/preserve-time	manter último registro de acesso

Códigos de saída

0	nenhuma ameaça encontrada
1	ameaça encontrada e removida
10	alguns arquivos não puderam ser rastreados (podem conter ameaças)
50	ameaça encontrada
100	erro

OBSERVAÇÃO: Os códigos de saída maiores que 100 significam que o arquivo não foi rastreado e, portanto, pode estar infectado.

3.9.5 Detecção em estado ocioso

As configurações de estado ocioso podem ser feitas em **Configuração avançada** em **Antivírus** > **Rastreamento em estado ocioso** > **Detecção em estado ocioso**. Essas configurações especificam um acionador para Rastreamento em estado ocioso, quando:

- a proteção de tela estiver em execução,
- o computador estiver bloqueado,
- um usuário efetuar logoff.

Use as opções de cada estado para ativar ou desativar os diferentes acionadores de detecção de estado ocioso.

3.9.6 ESET SysInspector

3.9.6.1 Introdução ao ESET SysInspector

O ESET SysInspector é um aplicativo que inspeciona completamente o seu computador e exibe os dados coletados de uma maneira abrangente. Informações como drivers e aplicativos instalados, conexões de rede ou entradas importantes de registro podem ajudá-lo a investigar o comportamento suspeito do sistema, seja devido a incompatibilidade de software ou hardware ou infecção por malware.

É possível acessar o ESET SysInspector de duas formas: Na versão integrada nas soluções ESET Security ou por meio de download da versão autônoma (SysInspector.exe) gratuita no site da ESET. Ambas as versões têm funções idênticas e os mesmos controles de programa. A única diferença é a forma como os resultados são gerenciados. As versões autônoma e integrada permitem exportar instantâneos do sistema em um arquivo *.xml* e salvá-los em disco. Entretanto, a versão integrada também permite armazenar os instantâneos do sistema diretamente em

Ferramentas > **ESET SysInspector** (exceto ESET Remote Administrator). Para mais informações, consulte a seção ESET SysInspector como parte do ESET Endpoint Security.

Aguarde enquanto o ESET SysInspector rastreia o computador. Pode demorar de 10 segundos a alguns minutos, dependendo da configuração de hardware, do sistema operacional e da quantidade de aplicativos instalados no computador.

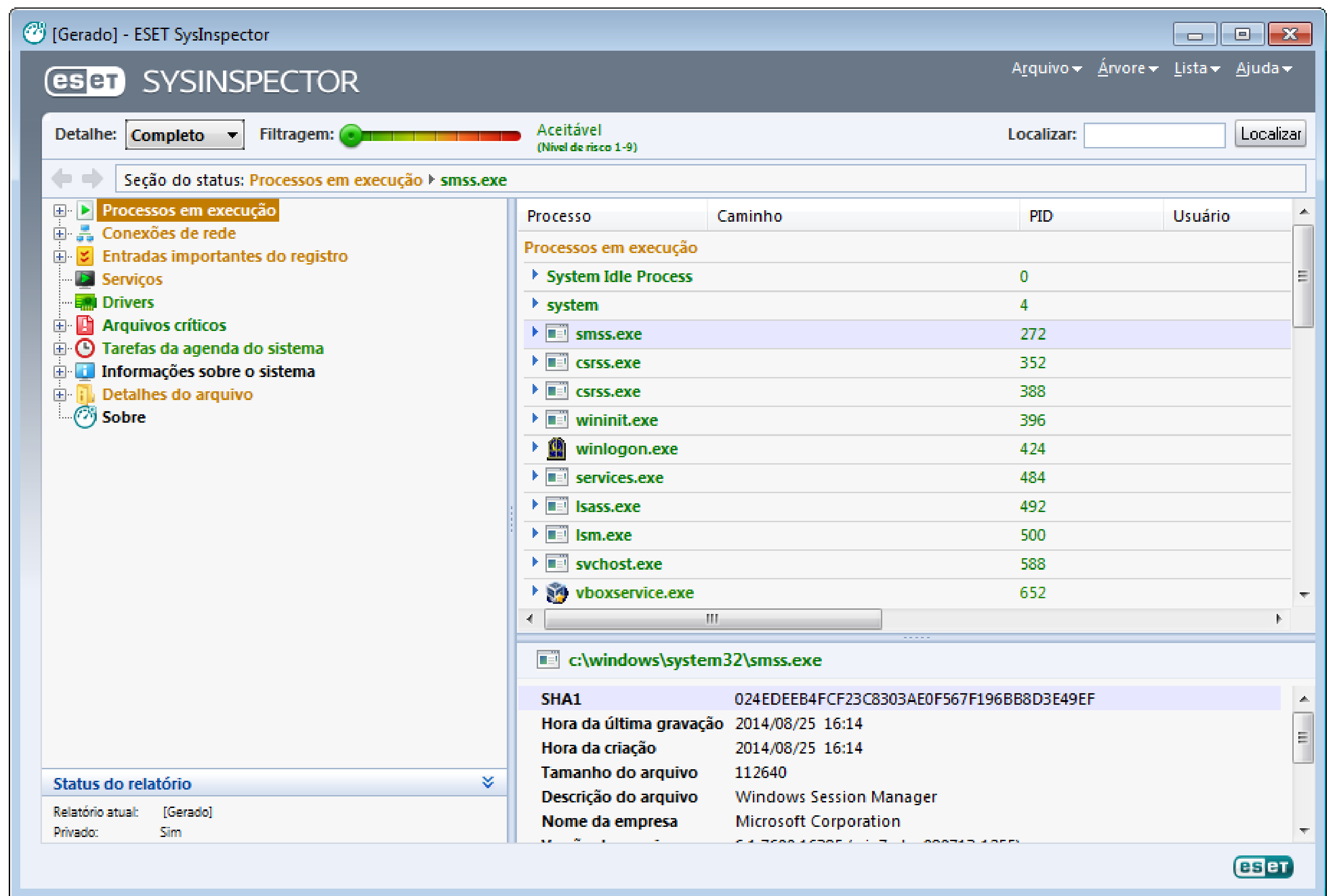
3.9.6.1.1 Inicialização do ESET SysInspector

Para iniciar o ESET SysInspector, basta executar o arquivo executável *SysInspector.exe* obtido por download no site da ESET. Se já tiver uma das soluções ESET Security instalada, é possível executar o ESET SysInspector diretamente a partir do menu Iniciar (clique em **Programas** > **ESET** > **ESET Endpoint Security**).

Aguarde enquanto o aplicativo inspeciona o sistema, o que pode demorar vários minutos.

3.9.6.2 Interface do usuário e uso do aplicativo

Para maior clareza, a janela do programa principal é dividida em quatro seções principais - Controles do programa localizados na parte superior da janela do programa principal, a janela Navegação à esquerda, a janela Descrição à direita e a janela Detalhes, na parte inferior da janela do programa principal. A seção Status do log lista os parâmetros básicos de um log (filtro usado, tipo de filtro, se o log é o resultado de uma comparação, etc.).



3.9.6.2.1 Controles do programa

Esta seção contém a descrição de todos os controles do programa disponíveis no ESET SysInspector.

Arquivo

Clicando em **Arquivo**, você pode armazenar o status atual do sistema para investigação posterior ou abrir um log armazenado anteriormente. Por motivo de publicação, recomendamos a geração de um log **Adequado para envio**. Neste formulário, o log omite informações confidenciais (nome do usuário atual, nome do computador, nome do domínio, privilégios do usuário atual, variáveis do ambiente, etc.).

OBSERVAÇÃO: Você pode abrir os relatórios do ESET SysInspector armazenados anteriormente arrastando e soltando-os na janela do programa principal.

Árvore

Permite expandir ou fechar todos os nós e exportar as seções selecionadas para o script de serviços.

Lista

Contém funções para uma navegação mais fácil dentro do programa e diversas outras funções, como, por exemplo, encontrar informações online.

Ajuda

Contém informações sobre o aplicativo e as funções dele.

Detalhe

Esta configuração influencia as informações exibidas na janela do programa principal para facilitar o trabalho com as informações. No modo "Básico", você terá acesso a informações utilizadas para encontrar soluções para problemas comuns no seu sistema. No modo "Médio", o programa exibe detalhes menos usados. No modo "Completo", o ESET SysInspector exibe todas as informações necessárias para resolver problemas muito específicos.

Filtragem

A filtragem de itens é mais adequada para encontrar arquivos suspeitos ou entradas do registro no sistema. Ajustando o controle deslizante, você pode filtrar itens pelo nível de risco deles. Se o controle deslizante estiver configurado todo para a esquerda (Nível de risco 1), todos os itens serão exibidos. Se você mover o controle deslizante para a direita, o programa filtrará todos os itens menos perigosos que o nível de risco atual e exibirá apenas os itens que são mais suspeitos que o nível exibido. Com o controle deslizante todo para a direita, o programa exibirá apenas os itens perigosos conhecidos.

Todos os itens identificados como de risco 6 a 9 podem colocar a segurança em risco. Se você não estiver utilizando uma solução de segurança da ESET, recomendamos que você rastreie o sistema com o ESET Online Scanner se o ESET SysInspector encontrou esse item. O ESET Online Scanner é um serviço gratuito.

OBSERVAÇÃO: O nível de risco de um item pode ser rapidamente determinado comparando a cor do item com a cor no controle deslizante Nível de risco.

Comparar

Ao comparar dois logs, você pode optar por exibir todos os itens, exibir apenas os itens adicionados, exibir apenas os itens removidos ou exibir apenas os itens substituídos.

Localizar

A opção Pesquisar pode ser utilizada para encontrar um item específico pelo nome ou por parte do nome. Os resultados da solicitação da pesquisa são exibidos na janela Descrição.

Retornar

Clicando na seta para trás e para a frente, você pode retornar para as informações exibidas anteriormente na janela Descrição. Você pode usar as teclas Backspace e de espaço em vez de clicar para trás e para a frente.

Seção do status

Exibe o nó atual na janela Navegação.

Importante: Os itens realçados em vermelho são desconhecidos, por isso o programa os marca como potencialmente perigosos. Se um item estiver em vermelho, isso não significa automaticamente que você pode excluir o arquivo. Antes de excluir, certifique-se de que os arquivos são realmente perigosos ou desnecessários.

3.9.6.2.2 Navegação no ESET SysInspector

O ESET SysInspector divide vários tipos de informações em diversas seções básicas chamadas de nós. Se disponíveis, você pode encontrar detalhes adicionais expandindo cada nó em seus subnós. Para abrir ou recolher um nó, clique duas vezes no nome do nó ou clique em ⊞ ou em ⊟ próximo ao nome do nó. À medida que percorrer a estrutura em árvore dos nós e subnós na janela Navegação, você pode encontrar diversos detalhes para cada nó mostrado na janela Descrição. Se você percorrer os itens na janela Descrição, detalhes adicionais sobre cada item podem ser exibidos na janela Detalhes.

A seguir estão as descrições dos nós principais na janela Navegação e as informações relacionadas nas janelas Descrição e Detalhes.

Processos em execução

Esse nó contém informações sobre aplicativos e processos em execução no momento da geração do log. Na janela Descrição, você pode encontrar detalhes adicionais para cada processo, como, por exemplo, bibliotecas dinâmicas usadas pelo processo e o local delas no sistema, o nome do fornecedor do aplicativo, o nível de risco do arquivo, etc.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

OBSERVAÇÃO: Um sistema operacional consiste em diversos componentes kernel importantes que são executados constantemente e que fornecem funções básicas e vitais para outros aplicativos de usuários. Em determinados casos, tais processos são exibidos na ferramenta ESET SysInspector com o caminho do arquivo começando com \??\. Esses símbolos fornecem otimização de pré-início para esses processos; eles são seguros para o sistema.

Conexões de rede

A janela Descrição contém uma lista de processos e aplicativos que se comunicam pela rede utilizando o protocolo selecionado na janela Navegação (TCP ou UDP), junto com os endereços remotos aos quais o aplicativo está conectado. Também é possível verificar os endereços IP dos servidores DNS.

A janela Detalhes contém informações adicionais dos itens selecionados na janela Descrição, como o tamanho do arquivo ou o hash dele.

Entradas importantes do registro

Contém uma lista de entradas de registro selecionadas que estão relacionadas freqüentemente a diversos problemas com o sistema, como aqueles que especificam os programas de inicialização, objetos auxiliares do navegador (BHO), etc.

Na janela Descrição, é possível localizar quais arquivos estão relacionados a entradas de registro específicas. Você pode consultar detalhes adicionais na janela Detalhes.

Serviços

A janela Descrição contém uma lista de arquivos registrados como serviços do Windows. É possível verificar a maneira como o serviço é configurado para iniciar, junto com detalhes específicos do arquivo na janela Detalhes.

Drivers

Uma lista de drivers instalados no sistema.

Arquivos críticos

A janela Descrição exibe o conteúdo dos arquivos críticos relacionados ao sistema operacional Microsoft Windows.

Tarefas da agenda do sistema

Contém uma lista de tarefas acionadas pela Agenda de Tarefas do Windows em uma hora/intervalo específico.

Informações do sistema

Contém informações detalhadas sobre hardware e software, além de informações sobre as variáveis ambientais configuradas, os direitos do usuário e os registros de eventos do sistema.

Detalhes do arquivo

Uma lista de arquivos importantes do sistema e arquivos na pasta Arquivos de programas. Informações adicionais específicas dos arquivos podem ser encontradas nas janelas Descrição e Detalhes.

Sobre

Informações sobre a versão do ESET SysInspector e a lista dos módulos do programa.

3.9.6.2.2.1 Atalhos do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET SysInspector incluem:

Arquivo

Ctrl+O	Abre o log existente
Ctrl+S	Salva os logs criados

Gerar

Ctrl+G	gera um instantâneo padrão do status do computador
Ctrl+H	gera um instantâneo do status do computador que também pode registrar informações confidenciais

Filtragem de itens

1, O	Aceitável, nível de risco 1-9, os itens são exibidos
2	Aceitável, nível de risco 2-9, os itens são exibidos
3	Aceitável, nível de risco 3-9, os itens são exibidos
4, U	Desconhecido, nível de risco 4-9, os itens são exibidos
5	Desconhecido, nível de risco 5-9, os itens são exibidos
6	Desconhecido, nível de risco 6-9, os itens são exibidos
7, B	Perigoso, nível de risco 7-9, os itens são exibidos
8	Perigoso, nível de risco 8-9, os itens são exibidos
9	Perigoso, nível de risco 9, os itens são exibidos
-	Diminui o nível de risco
+	Aumenta o nível de risco
Ctrl+9	Modo de filtragem, nível igual ou superior
Ctrl+0	Modo de filtragem, somente nível igual

Exibir

Ctrl+5	Exibição por fornecedor, todos os fornecedores
Ctrl+6	Exibição por fornecedor, somente Microsoft
Ctrl+7	Exibição por fornecedor, todos os outros fornecedores
Ctrl+3	Exibe detalhes completos
Ctrl+2	Exibe detalhes da mídia
Ctrl+1	Exibição básica
Backspace	Move um passo para trás
Espaço	Move um passo para a frente
Ctrl+W	Expande a árvore
Ctrl+Q	Recolhe a árvore

Outros controles

Ctrl+T	Vai para o local original do item após a seleção nos resultados de pesquisa
Ctrl+P	Exibe informações básicas sobre um item
Ctrl+A	Exibe informações completas sobre um item
Ctrl+C	Copia a árvore do item atual
Ctrl+X	Copia itens
Ctrl+B	Localiza informações sobre os arquivos selecionados na Internet
Ctrl+L	Abre a pasta em que o arquivo selecionado está localizado
Ctrl+R	Abre a entrada correspondente no editor do registro
Ctrl+Z	Copia um caminho para um arquivo (se o item estiver relacionado a um arquivo)
Ctrl+F	Alterna para o campo de pesquisa
Ctrl+D	Fecha os resultados da pesquisa
Ctrl+E	Executa script de serviços

Comparação

Ctrl+Alt+O	Abre o log original/comparativo
Ctrl+Alt+R	Cancela a comparação
Ctrl+Alt+1	Exibe todos os itens
Ctrl+Alt+2	Exibe apenas os itens adicionados; o log mostrará os itens presentes no log atual
Ctrl+Alt+3	Exibe apenas os itens removidos; o log mostrará os itens presentes no log anterior
Ctrl+Alt+4	Exibe apenas os itens substituídos (arquivos inclusive)
Ctrl+Alt+5	Exibe apenas as diferenças entre os logs
Ctrl+Alt+C	Exibe a comparação
Ctrl+Alt+N	Exibe o log atual
Ctrl+Alt+P	Exibe o log anterior

Diversos

F1	Exibe a Ajuda
Alt+F4	Fecha o programa
Alt+Shift+F4	Fecha o programa sem perguntar
Ctrl+I	Estatísticas de logs

3.9.6.2.3 Comparar

O recurso Comparar permite que o usuário compare dois logs existentes. O resultado desse recurso é um conjunto de itens não comuns a ambos os logs. Ele é adequado se você desejar manter controle das alterações no sistema, uma ferramenta útil para detectar código malicioso.

Após ser iniciado, o aplicativo criará um novo log, que será exibido em uma nova janela. Clique em **Arquivo** > **Salvar relatório** para salvar um log em um arquivo. Os arquivos de log podem ser abertos e visualizados posteriormente. Para abrir um log existente, clique em **Arquivo** > **Abrir relatório**. Na janela principal do programa, o ESET SysInspector sempre exibe um log de cada vez.

O benefício de comparar dois logs é que você pode visualizar um log ativo atual e um log salvo em um arquivo. Para comparar logs, clique em **Arquivo** > **Comparar relatório** e escolha **Selecionar arquivo**. O log selecionado será comparado com o log ativo na janela principal do programa. O log comparativo exibirá somente as diferenças entre esses dois logs.

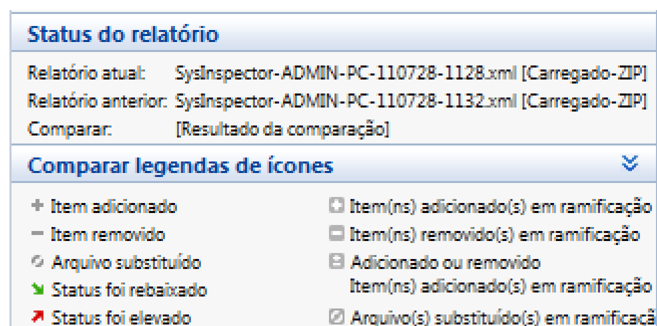
OBSERVAÇÃO: Caso compare dois arquivos de log, clique em **Arquivo** > **Salvar relatório** para salvá-lo como um arquivo ZIP; ambos os arquivos serão salvos. Se você abrir esse arquivo posteriormente, os logs contidos serão comparados automaticamente.

Próximo aos itens exibidos, o ESET SysInspector mostra símbolos que identificam diferenças entre os logs comparados.

Descrição de todos os símbolos que podem ser exibidos próximos aos itens:

- novo valor, não presente no log anterior
- a seção de estrutura em árvore contém novos valores
- valor removido, presente apenas no log anterior
- a seção de estrutura em árvore contém valores removidos
- o valor/arquivo foi alterado
- a seção de estrutura em árvore contém valores/arquivos modificados
- o nível de risco reduziu / era maior no log anterior
- o nível de risco aumentou / era menor no log anterior

A seção de explicação exibida no canto inferior esquerdo descreve todos os símbolos e também exibe os nomes dos logs que estão sendo comparados.



Qualquer log comparativo pode ser salvo em um arquivo e aberto posteriormente.

Exemplo

Gere e salve um relatório, registrando informações originais sobre o sistema, em um arquivo chamado previous.xml. Após terem sido feitas as alterações, abra o ESET SysInspector e deixe-o gerar um novo relatório. Salve-o em um arquivo chamado *current.xml*.

Para controlar as alterações entre esses dois logs, clique em **Arquivo** > **Comparar relatórios**. O programa criará um log comparativo mostrando as diferenças entre os logs.

O mesmo resultado poderá ser alcançado se você utilizar a seguinte opção da linha de comandos:

SysIsnpector.exe current.xml previous.xml

3.9.6.3 Parâmetros da linha de comando

O ESET SysInspector suporta a geração de relatórios a partir da linha de comando utilizando estes parâmetros:

/gen	gerar relatório diretamente a partir da linha de comando sem operar a GUI
/privacy	gerar relatório com informações confidenciais omitidas
/zip	salvar o relatório de resultado no arquivo zip compactado
/silent	suprimir a janela de progresso ao gerar o relatório da linha de comando
/blank	iniciar o ESET SysInspector sem gerar/carregar o relatório

Exemplos

Uso:
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Para carregar relatório específico diretamente no navegador, use: *SysInspector.exe .\clientlog.xml*
Para gerar relatório a partir da linha de comando, use: *SysInspector.exe /gen=.\mynewlog.xml*
Para gerar relatório excluindo informações confidenciais diretamente em um arquivo compactado, use: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Para comparar dois relatórios e procurar diferenças, use: *SysInspector.exe new.xml old.xml*

OBSERVAÇÃO: Se o nome do arquivo/pasta contiver uma lacuna, ele deve ser colocado entre aspas.

3.9.6.4 Script de serviços

O script de serviços é uma ferramenta que fornece ajuda aos clientes que utilizam o ESET SysInspector removendo facilmente os objetos indesejados do sistema.

O script de serviços permite que o usuário exporte o relatório completo do ESET SysInspector ou suas partes selecionadas. Após a exportação, você pode marcar os objetos não desejados para exclusão. Em seguida, você pode executar o log modificado para excluir os objetos marcados.

O script de serviços é adequado para usuários avançados com experiência anterior em diagnóstico de problemas do sistema. As modificações não qualificadas podem levar a danos no sistema operacional.

Exemplo

Se você suspeita que o seu computador está infectado por um vírus que não é detectado pelo seu programa antivírus, siga estas instruções passo a passo:

1. Execute o ESET SysInspector para gerar um novo instantâneo do sistema.
2. Selecione o primeiro item na seção à esquerda (na estrutura em árvore), pressione Shift e selecione o último item para marcar todos os itens.
3. Clique com o botão direito do mouse nos objetos selecionados e selecione **Exportar as seções selecionadas para script de serviços**.
4. Os objetos selecionados serão exportados para um novo log.
5. Esta é a etapa mais crucial de todo o procedimento: abra o novo log e altere o atributo - para + em todos os objetos que desejar remover. Verifique se não marcou arquivos/objetos do sistema operacional importantes.
6. Abra o ESET SysInspector, clique em **Arquivo** > **Executar script de serviços** e insira o caminho para o script.
7. Clique em **OK** para executar o script.

3.9.6.4.1 Geração do script de serviços

Para gerar um script, clique com o botão direito em um item na árvore de menus (no painel esquerdo) na janela principal do ESET SysInspector. No menu de contexto, selecione **Exportar todas as seções para script de serviços** ou **Exportar as seções selecionadas para script de serviços**.

OBSERVAÇÃO: Não é possível exportar o script de serviços quando dois logs estiverem sendo comparados.

3.9.6.4.2 Estrutura do script de serviços

Na primeira linha do cabeçalho do script, você pode encontrar informações sobre a versão do Mecanismo (ev), versão da GUI (gv) e a versão do log (lv). É possível usar esses dados para rastrear possíveis alterações no arquivo .xml que gera o script e evitar inconsistências durante a execução. Esta parte do script não deve ser alterada.

O restante do arquivo é dividido em seções nas quais os itens podem ser editados (refere-se àqueles que serão processadas pelo script). Marque os itens para processamento substituindo o caractere "-" em frente a um item pelo caractere "+". As seções no script são separadas das outras por uma linha vazia. Cada seção tem um número e um título.

01) Processos em execução

Esta seção contém uma lista de todos os processos em execução no sistema. Cada processo é identificado por seu caminho UNC e, subsequentemente, por seu código hash CRC16 em asteriscos (*).

Exemplo:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Neste exemplo, o processo, module32.exe, foi selecionado (marcado por um caractere "+"); o processo será encerrado com a execução do script.

02) Módulos carregados

Essa seção lista os módulos do sistema em uso no momento.

Exemplo:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Neste exemplo, o módulo khbekhb.dll foi marcado por um caractere "+". Quando o script for executado, ele reconhecerá os processos que usam esse módulo específico e os encerrará.

03) Conexões TCP

Esta seção contém informações sobre as conexões TCP existentes.

Exemplo:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

Quando o script for executado, ele localizará o proprietário do soquete nas conexões TCP marcadas e interromperá o soquete, liberando recursos do sistema.

04) Pontos de extremidade UDP

Esta seção contém informações sobre os pontos de extremidade UDP existentes.

Exemplo:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Quando o script for executado, ele isolará o proprietário do soquete nos pontos de extremidade UDP marcados e interromperá o soquete.

05) Entradas do servidor DNS

Esta seção contém informações sobre a configuração atual do servidor DNS.

Exemplo:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

As entradas marcadas do servidor DNS serão removidas quando você executar o script.

06) Entradas importantes do registro

Esta seção contém informações sobre as entradas importantes do registro.

Exemplo:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

As entradas marcadas serão excluídas, reduzidas ao valor de 0 byte ou redefinidas aos valores padrão com a execução do script. A ação a ser aplicada a uma entrada específica depende da categoria da entrada e do valor da chave no registro específico.

07) Serviços

Esta seção lista os serviços registrados no sistema.

Exemplo:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

Os serviços marcados e seus serviços dependentes serão interrompidos e desinstalados quando o script for executado.

08) Drivers

Esta seção lista os drivers instalados.

Exemplo:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Ao executar o script, os drivers selecionados serão parados. Observe que alguns drivers não permitirão serem parados.

09) Arquivos críticos

Esta seção contém informações sobre os arquivos que são críticos para o funcionamento correto do sistema operacional.

Exemplo:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Os itens selecionados serão excluídos ou redefinidos aos valores padrão originais.

3.9.6.4.3 Execução de scripts de serviços

Marque todos os itens desejados, depois salve e feche o script. Execute o script editado diretamente na janela principal do ESET SysInspector selecionando a opção **Executar script de serviços** no menu Arquivo. Ao abrir um script, o programa solicitará que você responda à seguinte mensagem: **Tem certeza de que deseja executar o script de serviços "%Scriptname%"?** Após confirmar a seleção, outro aviso pode ser exibido, informando que o script de serviços que você está tentando executar não foi assinado. Clique em **Executar** para iniciar o script.

Uma janela de diálogo confirmará que o script foi executado com êxito.

Se o script puder ser apenas parcialmente processado, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços foi executado parcialmente. Deseja exibir o relatório de erros?** Selecione **Sim** para exibir um relatório de erro complexo que lista as operações que não foram executadas.

Se o script não for reconhecido, uma janela de diálogo com a seguinte mensagem será exibida: **O script de serviços selecionado não está assinado. A execução de scripts não assinados e desconhecidos pode danificar seriamente os dados do computador. Tem certeza de que deseja executar o script e realizar as ações?** Isso pode ser causado por inconsistências no script (cabeçalho danificado, título da seção corrompido, ausência de linha vazia entre as seções, etc.). É possível reabrir o arquivo de script e corrigir os erros no script ou criar um novo script de serviços.

3.9.6.5 FAQ

O ESET SysInspector requer privilégios de administrador para ser executado?

Enquanto o ESET SysInspector não requer privilégios de administrador para ser executado, algumas das informações que ele coleta apenas podem ser acessadas a partir de uma conta do administrador. A execução desse programa como Usuário padrão ou Usuário restrito fará com que ele colete menos informações sobre o seu ambiente operacional.

O ESET SysInspector cria um arquivo de log?

O ESET SysInspector pode criar um arquivo de log da configuração do computador. Para salvar um arquivo de log, clique em **Arquivo** > **Salvar relatório** na janela do programa principal. Os arquivos de log são salvos em formato XML. Por padrão, os arquivos são salvos no diretório *%USERPROFILE%\My Documents*, com uma convenção de nomenclatura de arquivos de "SysInpsector-%COMPUTERNAME%-YYMMDD-HHMM.XML". Você pode alterar o local e o nome do arquivo de log para outro nome ou local antes de salvá-lo, se preferir.

Como visualizar o arquivo de log do ESET SysInspector?

Para visualizar um arquivo de log criado pelo ESET SysInspector, execute o programa e clique em **Arquivo** > **Abrir relatório** na janela do programa principal. Você também pode arrastar e soltar arquivos de log no aplicativo ESET SysInspector. Se você precisar visualizar os arquivos de log do ESET SysInspector com frequência, recomendamos a criação de um atalho para o arquivo SYSINSPECTOR.EXE na área de trabalho; é possível arrastar e soltar os arquivos de log para visualização. Por motivo de segurança, o Windows Vista/7 pode não permitir operações de arrastar e

soltar entre janelas que tenham permissões de segurança diferentes.

Há uma especificação disponível para o formato do arquivo de log? E um SDK?

Atualmente, não há uma especificação para o arquivo de log nem um SDK disponíveis, uma vez que o programa ainda está em desenvolvimento. Após o lançamento do programa, podemos fornecê-los com base nas informações fornecidas pelos clientes e sob demanda.

Como o ESET SysInspector avalia o risco representado por um objeto específico?

Na maioria dos casos, o ESET SysInspector atribui níveis de risco a objetos (arquivos, processos, chaves de registro e assim por diante), utilizando uma série de regras de heurística que examinam as características de cada objeto e determinam o potencial para atividade maliciosa. Com base nessa heurística, atribui-se um nível de risco aos objetos, que vai de 1 - Aceitável (verde) a 9 – Perigoso (vermelho). No painel de navegação esquerdo, as seções são coloridas com base no nível de risco mais alto de um objeto dentro delas.

Um nível de risco "6 - Desconhecido (vermelho)" significa que um objeto é perigoso?

As avaliações do ESET SysInspector não garantem que um objeto seja malicioso; essa determinação deve ser feita por um especialista em segurança. O ESET SysInspector é destinado a fornecer uma avaliação rápida para especialistas em segurança, para que eles saibam quais objetos em um sistema eles poderão querer examinar quanto a comportamento incomum.

Por que o ESET SysInspector conecta-se à Internet quando está em execução?

Como muitos aplicativos, o ESET SysInspector é assinado com um "certificado" de assinatura digital para ajudar a garantir que o software foi publicado pela ESET e que não foi alterado. Para verificar o certificado, o sistema operacional entra em contato com uma autoridade de certificação para verificar a identidade do editor do software. Esse é um comportamento normal para todos os programas assinados digitalmente no Microsoft Windows.

O que é a tecnologia Anti-Stealth?

A tecnologia Anti-Stealth proporciona a detecção efetiva de rootkits.

Se o sistema for atacado por um código malicioso que se comporte como um rootkit, o usuário poderá ser exposto à perda ou ao roubo de dados. Sem uma ferramenta especial anti-rootkit, é quase impossível detectar rootkits.

Por que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente ao mesmo tempo?

Ao tentar identificar a assinatura digital de um arquivo executável, o ESET SysInspector primeiro verifica se há uma assinatura digital incorporada no arquivo. Se uma assinatura digital for encontrada, o arquivo será validado usando essa informação. Se a assinatura digital não for encontrada, o ESI iniciará a procura do arquivo CAT (Security Catalog - *%systemroot%\system32\catroot*) correspondente que contenha informações sobre o arquivo executável processado. Caso o arquivo CAT relevante seja encontrado, sua assinatura digital será aplicada no processo de validação do executável.

É por isso que às vezes há arquivos marcados como "Assinado pela Microsoft", que têm uma entrada de "Nome da empresa" diferente.

3.9.6.6 ESET SysInspector como parte do ESET Endpoint Security

Para abrir a seção do ESET SysInspector no ESET Endpoint Security, clique em **Ferramentas** > **ESET SysInspector**. O sistema de gerenciamento na janela do ESET SysInspector é semelhante ao sistema dos relatórios de rastreamento do computador ou das tarefas agendadas. Todas as operações com instantâneos: criar, visualizar, comparar, remover e exportar podem ser acessadas com um ou dois cliques.

A janela do ESET SysInspector contém informações básicas sobre os snapshots criados, como a hora da criação, breve comentário, nome do usuário que criou o snapshot e o status do snapshot.

Para comparar, criar ou excluir instantâneos, utilize os botões correspondentes localizados abaixo da lista de instantâneos na janela do ESET SysInspector. Essas opções também estão disponíveis no menu de contexto. Para exibir o instantâneo do sistema selecionado, selecione **Mostrar** no menu de contexto. Para exportar o instantâneo

selecionado para um arquivo, clique com o botão direito e selecione **Exportar...**

Abaixo, veja uma descrição detalhada das opções disponíveis:

- **Comparar** - Permite comparar dois logs existentes. Ela é adequada se você desejar controlar alterações entre o log atual e um log anterior. Para que essa opção entre em vigor, é necessário selecionar dois instantâneos a serem comparados.
- **Criar...** - Cria um novo registro. Antes disso, é preciso inserir um breve comentário sobre o registro. Para saber mais sobre o progresso de criação de instantâneos (do instantâneo gerado no momento), consulte a coluna **Status**. Todos os instantâneos concluídos são marcados com o status **Criado**.
- **Excluir/Excluir tudo** - Remove as entradas da lista.
- **Exportar...** – Salva a entrada selecionada em um arquivo XML (também em uma versão compactada).

3.10 Glossário

3.10.1 Tipos de ameaças

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

3.10.1.1 Vírus

Um vírus de computador é uma parte de um código malicioso que é pré-anexado ou anexado a arquivos existentes no computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro. Quanto ao termo "vírus", ele é frequentemente usado de maneira incorreta para significar qualquer tipo de ameaça. Essa utilização está gradualmente sendo superada e substituída por um termo mais preciso "malware" (software malicioso).

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o código malicioso é chamado e executado antes da execução do aplicativo original. Um vírus pode infectar qualquer arquivo que tenha permissão de gravação dada pelo usuário.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositadamente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

Se o computador estiver infectado com um vírus e a limpeza não for possível, envie-o para o laboratório da ESET para análise. Em certos casos os arquivos infectados podem ser modificados a ponto de uma limpeza não ser possível e os arquivos precisarem ser substituídos por uma cópia limpa.

3.10.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se propagar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms propagam-se para os endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de horas ou mesmo minutos após sua liberação. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

3.10.1.3 Cavalos de Troia

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de ameaças que tentam se apresentar como programas úteis, enganando assim os usuários para executá-los.

Dado que Cavalos de Troia são uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- **Downloader** - Programas maliciosos com a capacidade de fazer o download de outras ameaças da Internet.
- **Dropper** - Programas maliciosos com a capacidade para instalar outros tipos de malware em computadores comprometidos.
- **Backdoor** - Programas maliciosos que se comunicam com atacantes remotos, permitindo que eles acessem o computador e assumam o seu controle.
- **Keylogger** - (keystroke logger) - Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- **Dialer** - Programas maliciosos projetados para se conectar aos números premium-rate em vez do provedor de serviços de Internet do usuário. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modens discados que não são mais usados regularmente.

Se um arquivo em seu computador for detectado como um cavalo de troia, é aconselhável excluí-lo, uma vez que ele contém códigos maliciosos.

3.10.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Há dois níveis de detecção para impedir rootkits:

1. Quando eles tentam acessar um sistema: Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).

2. Quando eles estão ocultos para os testes usuais: os usuários do ESET Endpoint Security têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

3.10.1.5 Adware

Adware é abreviação de “advertising-supported software” (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a homepage deste. O adware é frequentemente vinculado a programas freeware, permitindo que seus criadores cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso - os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Alguns programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há grande possibilidade de que contenha códigos maliciosos.

3.10.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de email da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O Spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável excluí-lo, uma vez que há grande probabilidade de ele conter códigos maliciosos.

3.10.1.7 Empacotadores

Empacotador é um executável de extração automática do tempo de execução que realiza vários tipos de malware em um único pacote.

Os empacotadores mais comuns são UPX, PE_Compact, PKLite e ASPack. O mesmo malware pode ser detectado de forma diferente quando compactado usando outro empacotador. Empacotadores também têm a capacidade de tornar suas "assinaturas" mutáveis ao longo do tempo, tornando o malware mais difícil de ser detectado e removido.

3.10.1.8 Aplicativos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET Endpoint Security fornece a opção de detectar tais ameaças.

Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não instalou), favor consultar o seu administrador de rede ou remover o aplicativo.

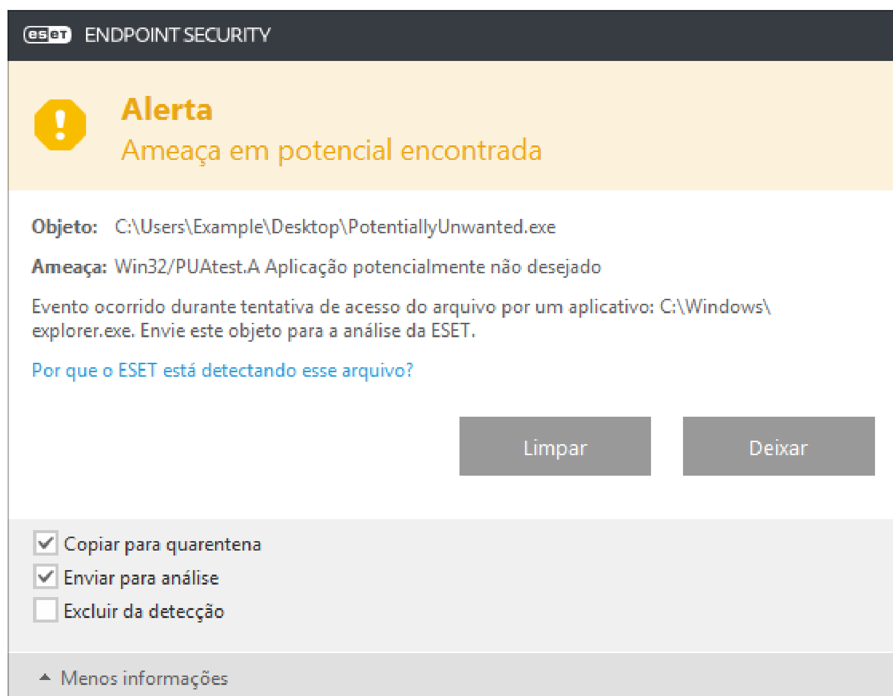
3.10.1.9 Aplicativos potencialmente indesejados

Um aplicativo potencialmente indesejado é um programa que contém adware, instala barras de ferramentas ou tem outros objetivos pouco claros. Existem algumas situações em um usuário pode sentir que os benefícios do aplicativo potencialmente indesejado superam os riscos. Por isso, a ESET atribui a estes aplicativos uma categoria de risco menor em comparação com outros tipos de software malicioso, como cavalos de Troia ou worms.

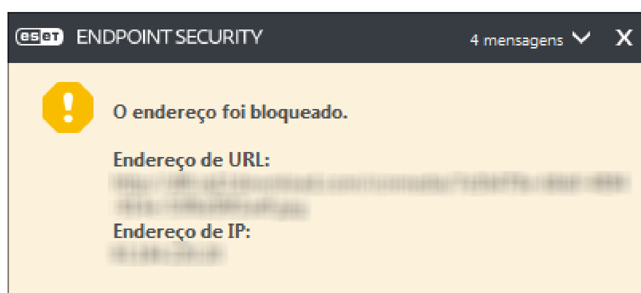
Aviso - Ameaça em potencial encontrada

Quando um aplicativo potencialmente indesejado é detectado, você poderá decidir qual ação realizar:

1. **Limpar/Desconectar**: Esta opção encerra a ação e evita que uma possível ameaça entre no sistema.
2. **Deixar**: Essa opção permite que a ameaça em potencial entre em seu sistema.
3. Para permitir que o aplicativo seja executado no seu computador no futuro sem interrupções, clique em **Mais informações/Exibir opções avançadas** e selecione a caixa de seleção ao lado de **Excluir da detecção**.

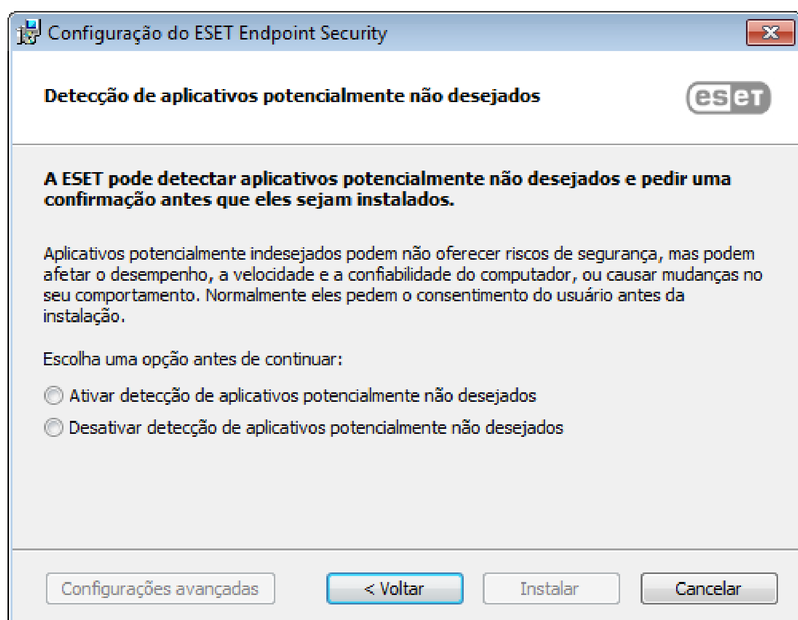


Quando um aplicativo potencialmente indesejado é detectado e não é possível limpar, uma janela de notificação **O endereço foi bloqueado** será exibida no canto inferior direito da tela. Para mais informações sobre este evento vá para **Ferramentas** > **Relatórios** > **Sites filtrados** no menu principal.



Aplicativos potencialmente indesejados - Configurações

Ao instalar seu produto ESET, é possível decidir se vai ativar a detecção de aplicativos potencialmente não desejados, conforme exibido abaixo:

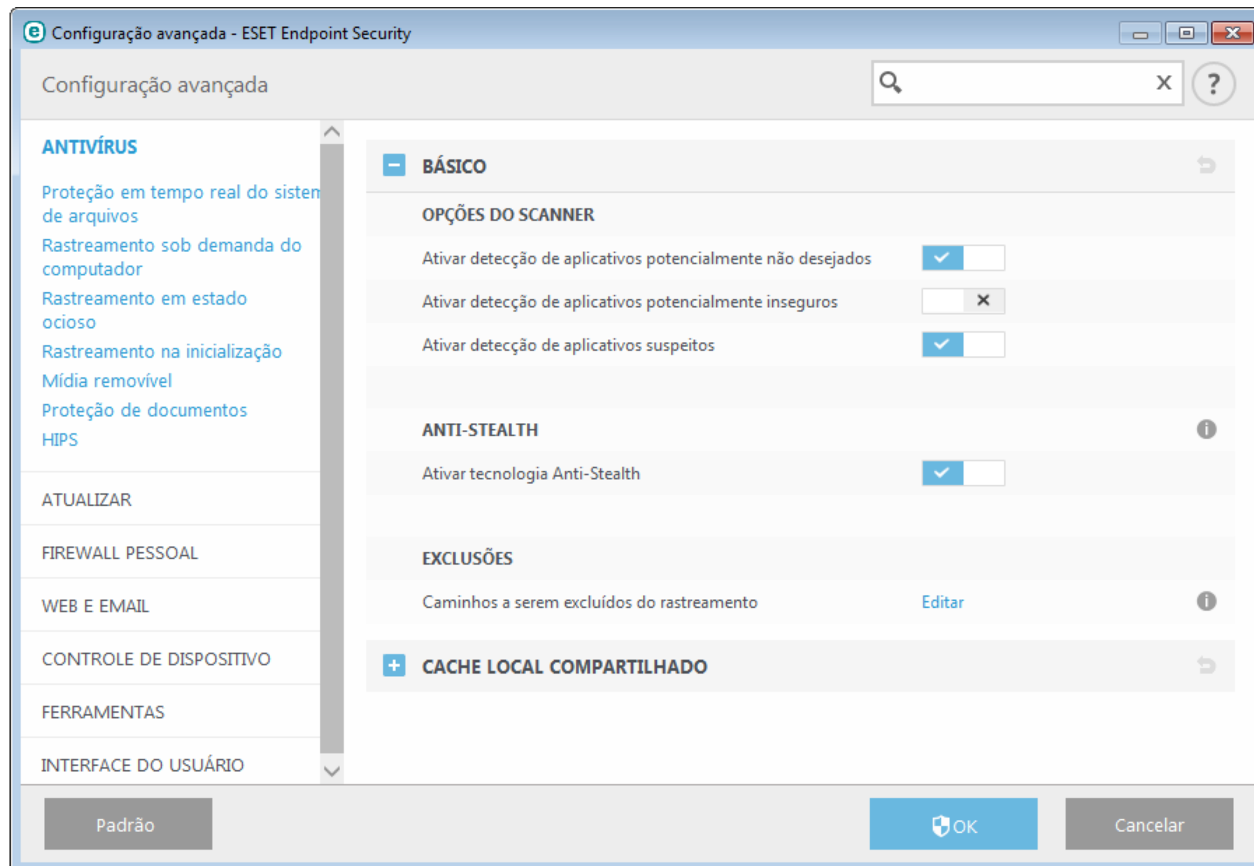


 Aplicativos potencialmente indesejados podem instalar adware, barras de ferramentas ou ter outros recursos

de programa indesejados e inseguros.

Essas configurações podem ser modificadas nas suas configurações de programa a qualquer momento. Para ativar ou desativar a detecção de Aplicativos potencialmente indesejados, inseguros ou suspeitos, siga essas instruções:

1. Abra seu produto ESET. Como abrir meu produto ESET?
2. Pressione a tecla **F5** para acessar a **Configuração avançada**.
3. Clique em **Antivírus** e ative ou desative as opções **Ativar detecção de aplicativos potencialmente não desejados**, **Ativar detecção de aplicativos potencialmente inseguros** e **Ativar detecção de Ativar detecção de aplicativos suspeitos** de acordo com suas preferências. Confirme clicando em **OK**.



Aplicativos potencialmente indesejados - Wrapper de software

Um wrapper de software é um tipo especial de modificação de aplicativo que é usado por alguns sites de hospedagem de arquivos. É uma ferramenta de terceiros que instala o programa que você planejou baixar, mas adiciona outros software, como barras de ferramentas ou adware. O software adicional também pode fazer alterações na página inicial do seu navegador ou nas configurações de pesquisa. Além disso, sites de hospedagem de arquivos muitas vezes não notificam o fabricante do software ou receptor do download que modificações foram feitas e não permite que seja possível optar por não obter uma modificação com facilidade. Por esses motivos, a ESET classifica wrapper de software como um tipo de aplicativo potencialmente indesejado para permitir aos usuários aceitarem ou não seu download.

Consulte o seguinte artigo da Base de Conhecimento ESET para obter uma versão atualizada desta página de ajuda.

3.10.1.10 Botnet

Um bot, ou um robô da web, é um programa de malware automatizado que rastreia blocos de endereços de rede e infecta computadores vulneráveis. Este tipo de programa permite que hackers tomem o controle de vários computadores ao mesmo tempo e transformem esses computadores em bots (também conhecido como um zumbi). Normalmente os hackers usam bots para infectar um grande número de computadores. Este grande grupo de computadores infectados é chamado de botnet. Quando um computador é infectado e se torna parte de um botnet, ele pode ser usado em ataques distribuídos de negação de serviço (DDoS), proxy e também podem ser usados para realizar tarefas automáticas na Internet sem o seu conhecimento (por exemplo: enviar spam, vírus ou roubar informações pessoais e particulares, como credenciais bancárias ou números de cartão de crédito).

3.10.2 Tipos de ataques remotos

Há muitas técnicas especiais que permitem que os agressores comprometam os sistemas remotos. Elas são divididas em diversas categorias.

3.10.2.1 Ataques de worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. Os worms da rede exploram as vulnerabilidades de segurança dos diversos aplicativos. Devido à disponibilidade da Internet, eles podem se espalhar por todo o mundo dentro de algumas horas após sua liberação.

A maioria dos ataques de worm podem ser evitados com o uso de configurações de segurança padrão no firewall. Além disso, é importante escolher o tipo de proteção **Rede pública** em redes públicas, bem como manter seu sistema operacional e programas atualizados com os patches de segurança mais recentes.

3.10.2.2 Ataques DoS

DoS, ou *Denial of Service* (negação de serviço), é a tentativa de impedir que o computador ou a rede sejam acessados por seus usuários. A comunicação entre os usuários afetados é obstruída e não pode mais continuar de modo funcional. Os computadores expostos aos ataques DoS geralmente precisam ser reinicializados para que voltem a funcionar adequadamente.

Na maioria dos casos, os alvos são servidores web e o objetivo é torná-los indisponíveis aos usuários por um determinado período de tempo.

3.10.2.3 Rastreamento de portas

O rastreamento de portas é usado para determinar se há portas abertas no computador em um host de rede. Um rastreador de porta é um software desenvolvido para encontrar tais portas.

Uma porta de computador é um ponto virtual que lida com os dados de entrada e saída - ação crucial do ponto de vista da segurança. Em uma rede grande, as informações reunidas pelos rastreadores de porta podem ajudar a identificar as vulnerabilidades em potencial. Tal uso é legítimo.

O rastreamento de porta é frequentemente usado pelos hackers na tentativa de comprometer a segurança. Seu primeiro passo é enviar pacotes para cada porta. Dependendo do tipo de resposta, é possível determinar quais portas estão em uso. O rastreamento por si só não causa danos, mas esteja ciente de que essa atividade pode revelar as vulnerabilidades em potencial e permitir que os agressores assumam o controle remoto dos computadores.

Os administradores de rede são aconselhados a bloquear todas as portas não usadas e proteger as que estão em uso contra o acesso não autorizado.

3.10.2.4 Envenenamento de DNS

Através do envenenamento de DNS (Domain Name Server), os hackers podem levar o servidor DNS de qualquer computador a acreditar que os dados falsos que eles forneceram são legítimos e autênticos. As informações falsas são armazenadas em cache por um determinado período de tempo, permitindo que os agressores reescrevam as respostas do DNS dos endereços IP. Como resultado, os usuários que tentarem acessar os websites da Internet farão o download de vírus ou worms no lugar do seu conteúdo original.

3.10.3 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. Flexível, rápido e direto, o email teve um papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com seus altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso - malware (códigos maliciosos). A inconveniência e o perigo para você são aumentados pelo fato de que os custos de envio são mínimos e os autores de spam têm muitas ferramentas para obter novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet
- Forneça seu email apenas a pessoas confiáveis
- Se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor
- Não responda a spam que já chegou à sua caixa de entrada
- Tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como "Sim, desejo receber informações".
- Use emails "especializados" – por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- De vez em quando, altere o seu email
- Utilize uma solução antispam

3.10.3.1 Propagandas

A propaganda na Internet é uma das formas de publicidade que mais cresce. As suas principais vantagens de marketing são o custo mínimo e um alto nível de objetividade. Além disso, as mensagens são enviadas quase que imediatamente. Muitas empresas usam as ferramentas de marketing por email para comunicar de forma eficaz com os seus clientes atuais e prospectivos.

Esse tipo de publicidade é legítimo, desde que você tenha interesse em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Nesses casos, a publicidade por email ultrapassa o limite razoável e se torna spam.

Hoje em dia a quantidade de emails não solicitados é um problema e não demonstra sinais de que vá diminuir. Geralmente, os autores dos emails não solicitados tentam mascarar o spam como mensagens legítimas.

3.10.3.2 Hoaxes

Um hoax é uma informação incorreta que é propagada pela Internet. Normalmente, os hoaxes são enviados por email ou por ferramentas de comunicação, como ICQ e Skype. A própria mensagem é geralmente uma brincadeira ou uma Lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes solicitam aos destinatários que encaminhem mensagens aos seus contatos, perpetuando-os. Há hoaxes de celular, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Na maioria dos casos, é impossível identificar a intenção do criador.

Se você receber uma mensagem solicitando que a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites especializados na Internet que podem verificar se o email é legítimo ou não.

Antes de encaminhar, faça uma pesquisa na Internet sobre a mensagem que você suspeita que seja um hoax.

3.10.3.3 Roubo de identidade

O termo roubo de identidade define uma atividade criminal que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados sensíveis como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (por exemplo instituição financeira, companhia de seguros). O email parecerá muito legítimo e conterá gráficos e conteúdo que podem vir originalmente da fonte pela qual ele está tentando se passar. Você será solicitado a digitar, sob várias pretensões (verificação dos dados, operações financeiras), alguns dos seus dados pessoais - números de contas bancárias ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, companhias de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

3.10.3.4 Reconhecimento de fraudes em spam

Geralmente, há alguns indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam.

- O endereço do remetente não pertence a alguém da sua lista de contatos.
- Você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma.
- Você é solicitado a inserir, sob vários pretextos (verificação de dados, operações financeiras), alguns de seus dados pessoais (números de contas bancárias, nomes de usuário e senhas, etc.)
- Está escrito em um idioma estrangeiro.
- Você é solicitado a comprar um produto no qual você não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original).
- Algumas das palavras estão com erros de ortografia em uma tentativa de enganar o seu filtro de spam. Por exemplo, "vaigra” em vez de “viagra”, etc.

3.10.3.4.1 Regras

No contexto das soluções antispam e dos clientes de email, as regras são as ferramentas para manipular as funções do email. Elas são constituídas por duas partes lógicas:

1. Condição (por exemplo, uma mensagem recebida de um determinado endereço)

2. Ação (por exemplo, a exclusão da mensagem, movendo-a para uma pasta especificada)

O número e a combinação de diversas regras com a solução antispam. Essas regras servem como medidas contra spam (email não solicitado). Exemplos típicos:

- 1. Condição: Uma mensagem de email recebida contém algumas palavras geralmente vistas nas mensagens de spam.
  2. Ação: Excluir a mensagem.

- 1. Condição: Uma mensagem de email recebida contém um anexo com a extensão .exe.
  2. Ação: Excluir o anexo e enviar a mensagem para a caixa de correio.

- 1. Condição: Uma mensagem de email recebida chega do seu patrão.
  2. Ação: Mover a mensagem para a pasta "Trabalho".

Recomendamos que você use uma combinação de regras nos programas antispam a fim de facilitar a administração e filtrar os spams com mais eficiência.

3.10.3.4.2 Lista de permissões

Em geral, uma lista de permissões é uma lista de itens ou pessoas que são aceites, ou para os quais foi concedida permissão de acesso. O termo "lista de permissões de email" define uma lista de contatos de quem o usuário deseja receber mensagens. Tais listas de permissões são baseadas nas palavras-chave para os endereços de email, nomes de domínio ou endereços IP.

Se uma lista de permissões funcionar de "modo exclusivo", então as mensagens de qualquer outro endereço, domínio ou endereço IP não serão recebidas. Se a lista de permissões não for exclusiva, tais mensagens não serão excluídas, mas filtradas de algum modo.

Uma lista de permissões baseia-se no princípio oposto de uma lista de proibições. As listas de permissões são relativamente fáceis de serem mantidas, mais do que as listas de proibições. Recomendamos que você use tanto a Lista de permissões como a Lista de proibições para filtrar os spams com mais eficiência.

3.10.3.4.3 Lista de proibições

Geralmente, uma lista de proibições é uma lista de itens ou pessoas proibidos ou inaceitáveis. No mundo virtual, é uma técnica que permite aceitar mensagens de todos os usuários não presentes em uma determinada lista.

Há dois tipos de lista de proibições: as criadas pelos usuários em seus aplicativos antispam e as listas de proibições profissionais atualizadas com frequência, criadas por instituições especializadas e que podem ser encontradas na Internet.

O uso dessas listas de proibições é um componente essencial da filtragem antispam bem-sucedida, mas é muito difícil mantê-la, uma vez que novos itens não bloqueados aparecem todos os dias. Recomendamos o uso de uma lista de permissões e uma lista de proibições para filtrar os spams com a maior eficácia.

3.10.3.4.4 Lista de exceções

A Lista de exceções geralmente contém endereços de email que podem ser falsificados e usados para o envio de spam. As mensagens de email de endereços relacionados na Lista de exceções serão sempre rastreadas quanto a spam. Por padrão, a Lista de exceções contém todos os endereços de email em contas existentes dos clientes de email.

3.10.3.4.5 Controle pelo servidor

O controle pelo servidor é uma técnica para identificar os emails de spam em massa com base no número de mensagens recebidas e nas reações dos usuários. Cada mensagem deixa uma "marca" digital única com base no conteúdo da mensagem. O número de ID único não diz nada sobre o conteúdo do email. Duas mensagens idênticas terão marcas idênticas, enquanto mensagens diferentes terão marcas diferentes.

Se uma mensagem for marcada como spam, sua marca será enviada ao servidor. Se o servidor receber mais marcas idênticas (correspondendo a uma determinada mensagem de spam), a marca será armazenada no banco de dados de marcas de spam. Ao rastrear as mensagens recebidas, o programa envia as marcas das mensagens ao servidor. O servidor retorna as informações sobre que marcas correspondem às mensagens já marcadas pelos usuários como spam.

3.10.4 Tecnologia ESET

3.10.4.1 Bloqueio de Exploit

O Bloqueio de Exploit é feito para fortalecer aplicativos comumente explorados como navegadores da web, leitores de PDF, clientes de email ou componentes do MS Office. Ele monitora o comportamento de processos em busca de atividades suspeitas que possam indicar um exploit. Ele adiciona outra camada de proteção, uma etapa mais avançada para proteção contra invasores, ao usar uma tecnologia totalmente diferente em comparação a técnicas com foco na detecção de arquivos maliciosos.

Quando o Bloqueio de Exploit identifica um processo suspeito, ele pode interromper o processo imediatamente e registrar os dados sobre a ameaça, que são enviados ao sistema de nuvem do ESET Live Grid. Estes dados poderão ser processados pelo Laboratório de Ameaças da ESET e usados para proteger melhor todos os usuários contra ameaças desconhecidas e ataques novos (de malware recém-lançado para o qual não há solução pré-configurada).

3.10.4.2 Rastreamento de memória avançado

O Rastreamento de memória avançado funciona junto com o Bloqueio de Exploit com o objetivo de fornecer uma melhor proteção contra malware desenvolvido para evitar a detecção por produtos antimalware através do uso de ofuscação e/ou criptografia. Em casos em que a emulação comum ou heurística podem não detectar uma ameaça, o Rastreamento de memória avançado é capaz de identificar o comportamento suspeito e rastrear ameaças conforme elas se revelam na memória do sistema. Esta solução é eficaz contra malware que ainda esteja fortemente ofuscado. Ao contrário do Bloqueio de Exploit, este é um método de pós-execução, o que significa que existe um risco de alguma atividade maliciosa possa ter sido realizada antes de uma ameaça ser detectada, porém no caso de outras técnicas de detecção terem falhado ele oferece uma camada adicional de segurança.

3.10.4.3 ESET Live Grid

Construído sobre o sistema de alerta precoce avançado ThreatSense.Net®, o ESET Live Grid usa dados que os usuários ESET enviaram em todo o mundo e envia-os para o Laboratório de vírus ESET. Ao fornecer amostras suspeitas e metadados originais, o ESET Live Grid nos permite reagir imediatamente às necessidades de nossos clientes e manter a ESET sensível às ameaças mais recentes. Pesquisadores de malware da ESET usam as informações para construir um instantâneo preciso sobre a natureza e abrangência das ameaças globais, que nos ajuda a concentrar nos alvos corretos. Os dados do ESET Live Grid desempenham um papel importante na definição de prioridades do nosso processamento automatizado.

Além disso, ele implementa um sistema de reputação que ajuda a melhorar a eficiência global de nossas soluções antimalware. Quando um arquivo executável está sendo inspecionado no sistema de um usuário, seu hashtag é comparado pela primeiro contra um banco de dados de itens na lista de permissões e lista de proibições. Se ele for encontrado na lista de permissões, o arquivo inspecionado é considerado limpo e sinalizado para ser excluído de rastreamentos futuros. Se ele estiver na lista de proibições as ações apropriadas serão tomadas com base na natureza da ameaça. Se nenhuma correspondência for encontrada o arquivo é verificado completamente. Com base nos resultados deste rastreamento, os arquivos são classificados como ameaças ou não ameaças. Esta abordagem tem um impacto positivo significante no desempenho do rastreamento.

Este sistema de reputação permite uma detecção eficaz de amostras de malware, mesmo antes de suas assinaturas serem distribuídas para usuários através de várias atualizações ao dia do banco de dados de vírus.

3.10.4.4 Proteção contra botnet

A proteção contra botnet descobre malware ao analisar seus protocolos de comunicação de rede. O botnet de malware é alterado frequentemente, em contraste com protocolos de rede, que não foram alterados nos últimos anos. Essa nova tecnologia ajuda a ESET a combater qualquer malware que tente conectar seu computador a uma rede botnet.

3.10.4.5 Bloqueio de Exploit do Java

O Bloqueio de Exploit do Java é uma extensão para a proteção de Bloqueio de Exploit ESET. Ela monitora o Java a procura de comportamentos semelhantes aos de exploit. Amostras bloqueadas podem ser encaminhadas para analisadores de malware, para que eles possam criar assinaturas para bloquear tentativas de exploit no Java em camadas diferentes (bloqueio de URL, download de arquivos, etc.).